sipri

MILITARY AND SECURITY DIMENSIONS OF QUANTUM TECHNOLOGIES

A Primer

MICHAL KRELINA

STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE

SIPRI is an independent international institute dedicated to research into conflict, armaments, arms control and disarmament. Established in 1966, SIPRI provides data, analysis and recommendations, based on open sources, to policymakers, researchers, media and the interested public.

The Governing Board is not responsible for the views expressed in the publications of the Institute.

STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE

Signalistgatan 9
SE-169 70 Solna, Sweden
Telephone: +46 8 655 97 00
Email: sipri@sipri.org
Internet: www.sipri.org

MILITARY AND SECURITY DIMENSIONS OF QUANTUM TECHNOLOGIES

A Primer

MICHAL KRELINA

July 2025

sipri

STOCKHOLM INTERNATIONAL
PEACE RESEARCH INSTITUTE

DOI: https://doi.org/10.55163/ZVTL1529

Contents

Acknowledgements

SIPRI and the author express their thanks to the government of Austria for its generous financial support for this publication.

The author is also grateful for the feedback provided by Sibylle Bauer, Alexander Blanchard, Mark Bromley, Lauriane Héau and Zeki C. Seskir. Finally, the author acknowledges the invaluable editorial work of the SIPRI Editorial Department.

Executive summary

Quantum technologies are moving rapidly from experimental laboratories to strategic domains, with significant implications for defence, security and international governance. Their distinctiveness lies not only in what they can compute or measure, but also in how they redefine access to knowledge—affecting encryption, sensing, timing and decision-making infrastructures.

The potential military relevance of quantum systems has attracted growing attention from alliances such as the North Atlantic Treaty Organization (NATO), from national governments and from multilateral initiatives. Significant capabilities include secure communication (via quantum key distribution, QKD), precise navigation without a global navigation satellite system (GNSS), highly sensitive detection and—eventually—quantum-enhanced computing. However, these technologies remain at varying stages of maturity and deployment. Many systems still face fundamental engineering hurdles, including scalability and error correction.

China and the European Union (EU) are leading the early deployment of quantum-secure networks and satellite-based QKD, marking the start of real-world experimentation.

In quantum computing, progress has been rapid but uneven. Experimental demonstrations have approached quantum supremacy (i.e. solving a specific, artificially constructed task, regardless of its practical usefulness), but practical quantum advantage (i.e. where a quantum device outperforms classical ones on meaningful problems) has not yet been conclusively achieved. Experts suggest that this milestone could arrive within one to three years, although this will depend on improvements in fidelity, error correction and algorithmic development. The implications of this progress span chemistry, optimization, logistics and machine learning, with long-term potential to influence cryptography and simulation of quantum systems.

A critical security concern is the risk to public-key cryptography. Once large-scale, universal quantum computers are operational, commonly used encryption methods such as Rivest–Shamir–Adleman (RSA) and elliptic curve cryptography (ECC) could be broken. This is not only a future concern: encrypted data can already be intercepted and stored for future decryption—the so-called harvest-now, decrypt-later strategy. In response, governments and standards bodies are preparing post-quantum cryptographic (PQC) algorithms to safeguard digital infrastructure. QKD may supplement these defences in applications that require high levels of assurance.

Quantum sensing technologies are closer to field deployment. They offer benefits such as location tracking without satellites, detection of subterranean or underwater assets, and improved precision in radar and timing. Such capabilities are already being tested for military navigation and surveillance, especially in GNSS-denied environments. These systems depend heavily on magnetic and gravity anomaly data sets, which are becoming increasingly valuable as strategic geospatial infrastructure.

The international governance landscape for quantum is still emerging. Many national strategies have been launched since 2021, with sharp growth in 2023–25. Most focus on research, infrastructure, talent and industrial policy, but several now explicitly include security and cryptography. Moreover, the reliance of quantum systems on specialized components makes supply chain resilience a growing focus of national strategies. Multilateral coordination remains fragmented. Export controls, the setting of standards, and the development of norms are influenced by geopolitical competition. For instance, debates within the International Organization for Standardization (ISO) and the International Telecommunication Union (ITU) over QKD protocols reveal how quantum standardization may become a strategic battleground. Policymakers should ensure that

emerging governance structures balance innovation incentives with safeguards against fragmentation or misuse.

The dual-use nature of quantum technologies—where civilian advances can be rapidly applied to military or intelligence contexts—is a recurring theme throughout this field. Attempts to fully separate military and civilian development are likely to fail. Regulatory responses therefore focus on responsible governance of technologies with dual civil and military applications, on export control and on ethical guidance. Several countries, international organizations and alliances are exploring oversight models to manage this balance.

The proliferation of open-source quantum tools and declining hardware costs raise the possibility of non-state actors gaining access to these technologies in the future. While near-term risks remain low, early engagement with law enforcement and technical regulators is warranted. Agencies such as the International Criminal Police Organization (Interpol) and the EU Agency for Law Enforcement Cooperation (Europol) have begun developing guidance and early-warning systems for future quantum misuse.

Despite growing interest in the strategic implications of quantum technologies, there is currently a lack of dedicated institutions that focus on assessing quantum's impact on peace and security. Existing ethical and societal initiatives rarely address arms control, deterrence or dual-use risks. Experts and policymakers have called for the creation of observatories, research centres or international bodies to fill this gap.

In conclusion, quantum technologies are reshaping the global security landscape not through brute force, but by altering how information is sensed, shared and secured. Their trajectory will be defined not only by scientific progress but also by policy frameworks, ethical norms and international cooperation. The goal is not to control quantum's development, but to ensure that it strengthens rather than destabilizes global peace and security.

Abbreviations

AI	Artificial intelligence
AUKUS	Trilateral Australia–United Kingdom–United States security agreement
BCI	Brain–computer interface
BSI	Bundesamt für Sicherheit in der Informationstechnik (German Federal Office for Information Security)
C4ISR	Command, control, communications, computers, intelligence, surveillance and reconnaissance
CRQC	Cryptographically relevant quantum computer
ECC	Elliptic curve cryptography
EDF	European Defence Fund
ENISA	European Union Agency for Cybersecurity (formerly European Network and Information Security Agency)
EU	European Union
Europol	European Union Agency for Law Enforcement Cooperation
EuroQCI	European Quantum Communication Infrastructure
GNSS	Global navigation satellite system
GPS	Global Positioning System
He-3	Helium-3
IEC	International Electrotechnical Commission
INS	Inertial navigation system
Interpol	International Criminal Police Organization
IP	Intellectual property
ISO	International Organization for Standardization
IT	Information technology
ITU	International Telecommunication Union
ITU-T	Telecommunication Standardization Sector of the International Telecommunication Union
JTC	Joint technical committee
MEG	Magnetoencephalography
NATO	North Atlantic Treaty Organization
NISQ	Noisy intermediate-scale quantum (device)
NIST	National Institute of Standards and Technology (United States)
NV	Nitrogen-vacancy (centre)
PLA	People's Liberation Army (China)
PNT	Positioning, navigation and timing
PQC	Post-quantum cryptographic
QDM	Quantum diamond microscope
QEC	Quantum error correction
QKD	Quantum key distribution
QPU	Quantum processing unit
QRNG	Quantum random number generator
R&D	Research and development
RF	Radio-frequency
RSA	Rivest–Shamir–Adleman (algorithm)
SCA	Side-channel attack
SCA-QS	Side-Channel Attacks with Quantum Sensing (project)
SSBN	Nuclear-powered ballistic missile submarine
SWaP-C	Size, weight, power and cost
UAV	Uncrewed aerial vehicle

UN	United Nations
UNIDIR	United Nations Institute for Disarmament Research
WMD	Weapons of mass destruction

1. Introduction

Quantum technologies have placed humanity at a historic crossroads. Past breakthroughs in physics have often redefined both the battlefield and the global order: from the internal combustion engine to nuclear fission; from radar to satellite navigation. Quantum is part of this tradition. But, unlike past revolutions that reshaped physical force or firepower, quantum technologies do not merely offer new tools; they challenge prevailing conceptions about information, time, space and causality. Like the digital revolution before it, the quantum shift is primarily about knowledge—how the world is sensed, how to protect data, how to make decisions and how to coordinate across distance. For instance, quantum technologies can enable ultra-secure communications networks or radically improve the optimization of complex systems like global supply chains.

As quantum technologies move quickly from research laboratories into real-world applications in computing, communications, sensing and navigation, they are having major implications for security and defence. Governments, militaries and strategic alliances around the world are increasingly focused on quantum tools as potential game changers in both civilian and military domains. These developments, and the choice of road to follow, raise complex strategic and ethical questions. Early acquisition or unexpected use of quantum capabilities by certain actors could introduce new forms of strategic asymmetry. The pursuit of quantum advantage—where a quantum device outperforms classical ones on meaningful problems—may either accelerate a new technological arms race or, alternatively, may foster cooperation through shared standards and secure communications. Ensuring alignment between quantum development, democratic values and long-term human interests presents a critical governance challenge.

What is clear already is that quantum has entered the strategic imagination. The North Atlantic Treaty Organization (NATO) has warned that 'quantum technologies have the potential for a revolutionary impact on NATO operations'.[1] The European Union (EU) sees them as a core part of digital sovereignty and strategic importance and is investing in secure quantum infrastructure across its territory, an ambition soon to be reinforced by the forthcoming EU strategy and act.[2] China has made military applications a clear priority, with the People's Liberation Army (PLA) recognizing the 'strategic significance and operational potential of quantum technologies in [its] attempts to achieve a decisive advantage'.[3] India's Ministry of Defence has highlighted the strategic stakes, stating that: 'Quantum technology has a huge potential for military application and a disruptive impact on modern-day warfare.'[4]

This primer provides a non-technical guide to understanding the relationship between quantum technologies and international security. It outlines how quantum science connects to military capabilities, what strategic advantages may emerge and what policy challenges lie ahead. The objective is to offer the reader a clear overview

[1] Reding, D. F. et al., *Science & Technology Trends 2023–2043*, vol. 1, *Overview* (NATO Science & Technology Organization, Mar. 2023), p. 58.

[2] European Commission, *Horizon Europe: Work Programme 2021–2022*, part 7, *Digital, Industry and Space* (European Commission: Brussels, 15 June 2021), p. 210; and European Commission, 'A competitiveness compass for the EU', Communication to the European Parliament etc., COM(2025) 30 final, 29 Jan. 2025.

[3] Kania, E. and Costello, J., 'Quantum leap (part 2): The strategic implications of quantum technologies', *China Brief*, vol. 16, no. 19 (21 Dec. 2016).

[4] Indian Ministry of Defence (MOD), 'MoD all set to take a leap in quantum communication technology to celebrate "Azadi Ka Amrit Mahotsav" [Elixir festival of independence]', Press Information Bureau, 14 Aug. 2022. See also Nikolayev, P. and Panda, S., *India's Quantum Technology Ecosystem: 2022–2023* (Aspen Quantum Consulting: Towson, MD, Dec. 2023), p. 9.

of the opportunities, risks and emerging trends—without requiring a background in physics or engineering.

It is important to note that, while the potential of quantum technologies is real, much of the public discussion has been shaped by hype, simplification or fear. Some claims exaggerate the current capabilities of quantum devices, while others overlook the real breakthroughs that are happening. This primer seeks to present a balanced tone: highlighting strategic developments and possible impacts, but also being honest about technical limits and timelines.

This primer does not aim to predict the future. It focuses on mapping the terrain—exploring how quantum technologies intersect with defence, security and policy. The intention is to support informed thinking, sober planning and responsible development in a field that could shape the foundations of global power in the decades ahead.

It continues in chapter 2 with an outline of the fundamentals of quantum technologies, with chapter 3 identifying specifically military applications of these technologies. The focus shifts in chapter 4 to their role in international security and in chapter 5 to national and international strategic approaches. Finally, chapter 6 describes national and multilateral governance of and through quantum technologies, before the paper concludes in chapter 7 with a series of recommendations. Appendix A provides a glossary of common terms related to quantum technologies.

2. Quantum technology fundamentals

The science of quantum mechanics began in the early 20th century, around the year 1900. It originated when scientists such as Max Planck and Albert Einstein began studying how energy behaves in tiny particles like atoms and light. Their discoveries showed that the natural world behaves in surprising ways at small scales—very different from what is seen in everyday life. This period marked the beginning of quantum science.[5]

Over the following decades, this scientific understanding continued to develop, as more scientists explored the strange and powerful rules of the quantum realm. This progress led to the first quantum revolution, which took place between the 1920s and 1960s. During this time, theoretical advances were translated into practical technologies, resulting in inventions such as the laser, the transistor and the atomic clock—all of which still play an important role in the modern world. These breakthroughs showed how quantum science could be used to create real-world tools, laying the foundation for many technologies currently in use.

The most powerful and world-changing result of the first quantum revolution was the development of nuclear weapons: the understanding of atomic structure made possible by quantum science led directly to the creation of the atomic bomb. This technology has shaped global security since it was first deployed during World War II. It was one of the first and most dramatic examples of how advances in quantum science have influenced the balance of power on a global scale.

While the technologies of the first quantum revolution were based on the collective behaviour of large numbers of quantum particles—such as the flow of electrons in a semiconductor or the light waves in a laser—the field is now entering a new stage. This second quantum revolution goes deeper: it involves the ability to control and use individual quantum systems, such as single atoms, electrons or photons—these are what are often referred to as 'quantum technologies'. They give access to new effects that were not possible before, like superposition and entanglement, that are being applied in powerful new ways for sensing, communications and computing.

Quantum physics and information: A brief overview

At the heart of quantum physics is the idea of quanta—the smallest possible units of certain physical properties. In the quantum world, many things that seem smooth and continuous at macroscopic scale actually come in tiny, fixed steps. Properties such as the energy levels of an atom, the spin of an electron, or the polarization of a photon are quantized—they can only take on specific, well-defined values. These discrete, controllable states make quantum systems uniquely suited for encoding and manipulating information. This is the foundation of quantum technologies: using nature's fundamental units as tools for sensing, secure communication and computation. Quantum information science builds on this by exploring how these quantized states can be harnessed to process information in ways that classical systems cannot.

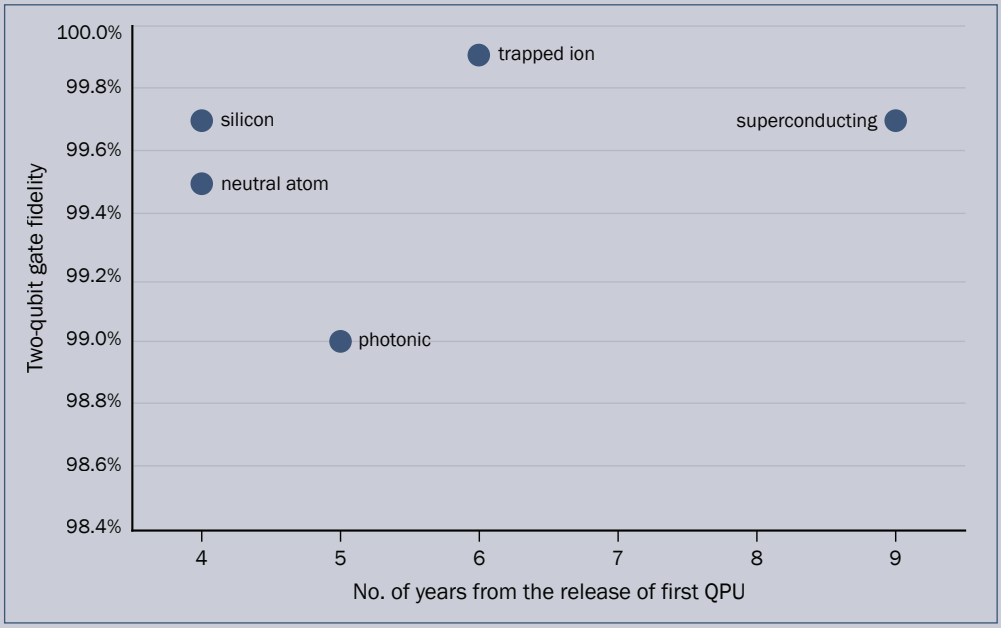
In this context, the basic unit of information is called a quantum bit or qubit. Like a classical bit, a qubit can represent 0 or 1—but, because of a uniquely quantum effect called superposition, a qubit can also be in a mixture of both states at once. This allows quantum systems to carry out tasks in ways that classical systems cannot. The qubit can be realized using many different physical systems, such as atoms, ions, photons or

[5] For a basic introduction to quantum physics see Susskind, L. and Friedman, A., *Quantum Mechanics: The Theoretical Minimum* (Basic Books: New York, 2014).

Box 2.1. Qubit technologies

Qubits can be realized through a variety of physical systems, each with its own advantages and trade-offs. Leading platforms today include superconducting qubits, used by companies like Google and IBM; trapped ion, known for high fidelity but slower quantum operations on qubits; and photonic qubits, which promise room-temperature operation and scalability. Neutral-atom qubits, where individual atoms are trapped and manipulated with lasers, offer excellent scalability and long coherence times. In addition, silicon-based spin qubits, compatible with existing semiconductor manufacturing processes, have gained attention for their compactness and potential integration with classical electronics.

While superconducting qubits are currently the most mature technology, with nearly a decade of development behind them, their progress has been incremental. In contrast, newer modalities such as silicon qubits have improved rapidly in a shorter time frame (see the figure below), challenging earlier expectations regarding long-term technological leadership. However, it is worth noting that superconducting platforms have scaled to systems with hundreds of reliable qubits, while spin qubit systems currently operate with around 10 qubits—highlighting a significant gap in overall system maturity. At this stage, it remains unclear which qubit platform will ultimately lead to scalable, fault-tolerant quantum computing; it is plausible that multiple modalities will coexist or even be integrated in future hybrid systems.



Comparative fidelity of two-qubit operations across quantum hardware platforms

This figure illustrates the improvement of two-qubit gate fidelity as a benchmark for quantum computing across various hardware platforms: neutral-atom, silicon, photonic, trapped-ion and superconducting qubits. Two-qubit gates enable entanglement, a critical feature for running quantum algorithms. The vertical axis shows the highest reported fidelity (in %), while the horizontal axis marks years since each platform's first quantum processing unit (QPU) was released. The figure illustrates both the progress and relative maturity of each platform over time.

In quantum computing, fidelity is a measure of how close a quantum state or operation is to its ideal or expected version. It quantifies the accuracy of quantum processes, such as gate operations or state preparation. A fidelity of 1 or 100% means perfect agreement with the target state or operation, while lower values indicate deviations due to noise, errors or imperfections.

Source: Quantum Insider, 'Quantum processors', accessed 13 Apr. 2025.

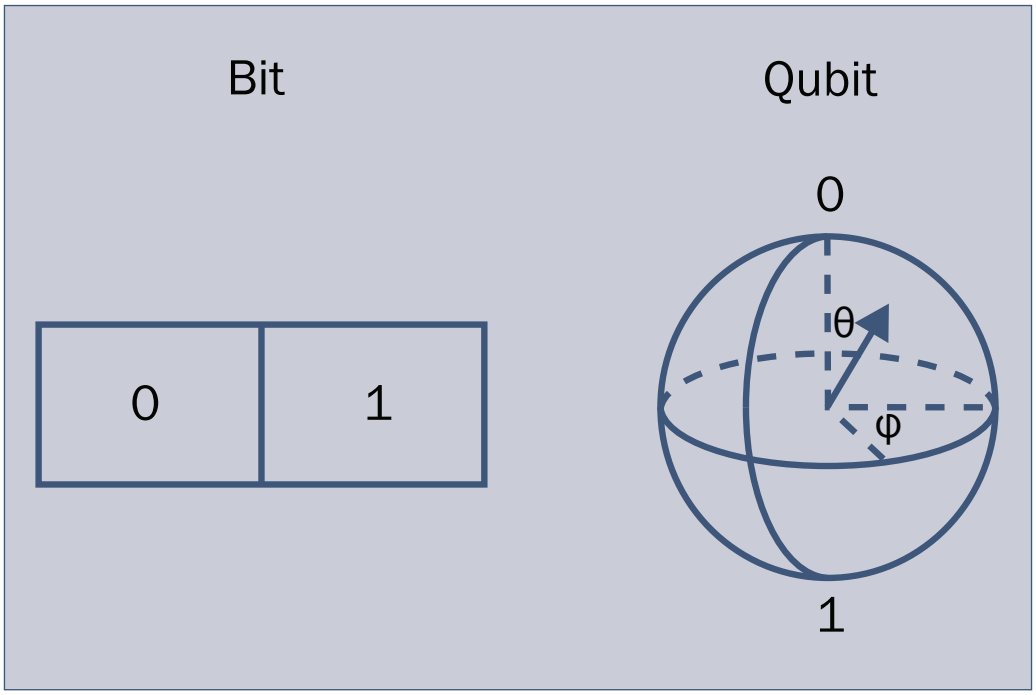


Figure 2.1. Visual comparison of classical and quantum bits

A classical bit can be in one of two states, 0 or 1. In contrast, a qubit can exist in a superposition of both states, represented as any point on the surface of the Bloch sphere. The direction of the vector shows the exact combination of 0 and 1, determined by two angles, θ and φ. This ability to occupy a continuum of states is what gives quantum systems their unique power.

tiny superconducting circuits cooled to near absolute zero (see box 2.1). It is a central concept in today's quantum information science.

Two key principles make qubits powerful: superposition and entanglement. Superposition means that a qubit can be in a combination of the 0 and 1 states at the same time, not just one or the other (see figure 2.1). This can be compared to a coin spinning in the air—until it lands, it is not only heads or tails, but both. In a quantum computer with multiple qubits, this allows many possible outcomes to be explored at once, offering potential computational advantages for specific problems.

Entanglement is another uniquely quantum effect. When two qubits become entangled, the state of one is directly connected to the state of the other, no matter how far apart they are. The measurement of one provides immediate information about the other. This strange connection allows for new types of secure communication and powerful processing techniques that are impossible with classical systems.

One important detail about superposition is that not all possible states are directly observable at once. When a qubit is measured, the superposition 'collapses' into just one of the possible outcomes—either 0 or 1. This means that, while a quantum computer can explore many possibilities with multiple qubits at once, only a single result is obtained upon measurement. To understand the overall pattern or find the right answer, the same quantum algorithm is repeated many times, and the results are analysed statistically.

Despite the need for repetition, this approach still offers a major advantage. For example, while two classical bits can represent only one of four (i.e. 2^2) possible combinations at a time, two qubits in superposition can represent all four combinations simultaneously. With more qubits, this grows exponentially: n qubits can represent 2^n combinations (e.g. 10 qubits can represent 1024 combinations at once, as visualized in figure 2.2, and 20 can represent over a million). This parallelism underlies the

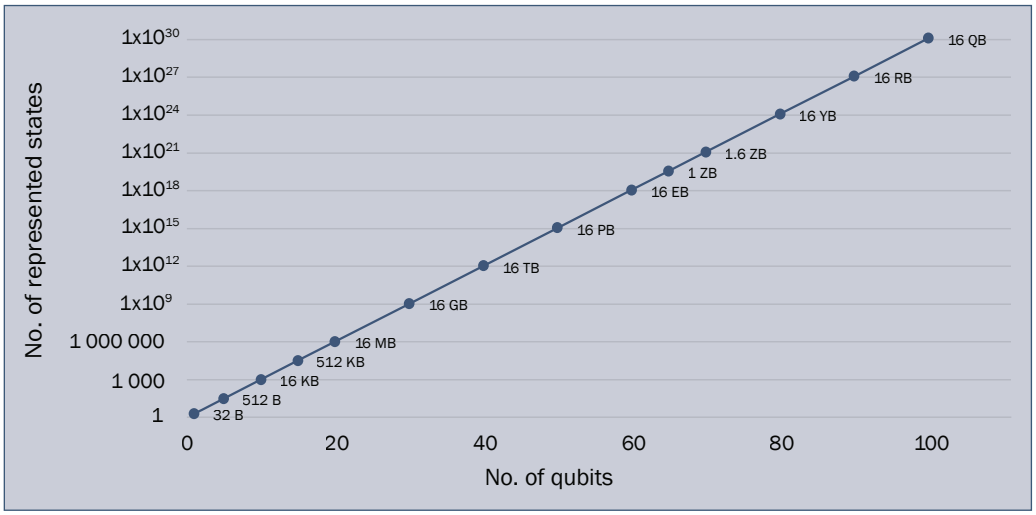


Figure 2.2. Growth of quantum state complexity and memory requirements

This graph shows how the number of quantum states doubles with each added qubit, following the formula 2^n, where n is the number of qubits. It also visualizes the classical memory (RAM) required to store these states, assuming that each state is represented as a complex number. For example, simulating 30 qubits already requires around 16 gigabytes (GB) of memory, while 50 qubits need over 16 petabytes (PB). Even combining the estimated total memory capacity of the planet—about 1 zettabyte (ZB)—would allow simulation of only around 65 qubits. This highlights the exponential growth of quantum complexity and the limits of classical computation.

computational potential of quantum systems, particularly for complex problems that are extremely hard for classical computers to solve.

These core quantum principles—superposition, entanglement and quantum measurement—are now being applied across three major areas of quantum technologies: computing, communications and sensing. In quantum computing, they enable machines that can solve certain complex problems much faster than classical computers. In quantum communications, superposition and entanglement allow for ultra-secure methods of sharing information, with the ability to detect any attempt at interception. And in quantum sensing, the extreme sensitivity of quantum systems is used to measure time, gravity or magnetic fields with precision far beyond what classical tools can achieve. Each of these fields is advancing rapidly, with potential applications in security, defence and critical infrastructure.

Quantum computing

The term quantum computing refers to devices that leverage the principles of quantum information to perform computations that offer potential advantages for specific classes of problems. These advantages may stem from features such as quantum superposition and entanglement, which allow quantum processors to tackle certain computational tasks more efficiently than their classical counterparts.

Quantum computing typically takes the form of universal quantum computers, which can solve a wide range of problems using quantum gates (quantum operations). These systems use either fixed qubits, which are stationary and manipulated by sequences of logic gates (gate-based model), or flying qubits, which are particles like photons that move through a circuit and are measured along the way (measurement-based model). In addition to universal machines, there are more specialized quantum devices, such as quantum annealers and quantum simulators: quantum annealers are designed to solve optimization problems by guiding a quantum system towards its lowest energy state, potentially exploiting quantum tunnelling to escape local minima, whereas quantum

simulators are specialized devices built to replicate and study specific quantum systems found in nature, such as molecular interactions.

There are multiple perspectives on how quantum computing fits into the broader landscape of computing. One particularly practical view is to consider quantum processing units (QPUs)—the core hardware units in a quantum computer—as specialized computational resources, much like the central processing unit (CPUs), graphics processing units (GPUs) or field-programmable gate arrays (FPGAs) in a classical system. In this context, QPUs serve as accelerators for specific tasks, particularly those involving quantum simulation, optimization or certain cryptography-breaking algorithms.

It is important to note that quantum computers are not meant to replace classical computers. In fact, every quantum computer today relies heavily on a classical system for a variety of essential functions: controlling the quantum hardware (e.g. pulse sequencing, calibration, error correction); running the classical parts of quantum algorithms (e.g. variational optimization); and interpreting results and presenting them in a human-readable format. This tight integration means that the future of computing is likely to be hybrid, combining classical and quantum resources in a cooperative architecture tailored to the nature of the computational problem being addressed. Hybrid architectures combine classical and quantum processors, with classical systems handling control, data input/output and error correction, while quantum processors are used as accelerators for specific subtasks such as simulation or optimization. This model, known as hybrid computing, uses quantum hardware only for targeted subtasks, with the classical computer performing the bulk of the computation and all orchestration tasks.

Quantum supremacy

One of the most discussed milestones in quantum computing is the concept of quantum supremacy.[6] This refers to the point at which a quantum computer can solve a specific problem that is infeasible for any classical computer, regardless of its practical usefulness. It is intended as a demonstration of quantum computational capability, rather than an application-driven breakthrough.

Quantum supremacy was first claimed by Google in 2019.[7] However, subsequent improvements to classical algorithms reduced the perceived advantage—problems initially described as taking 10 000 years on a classical supercomputer were later shown to be solvable in days.[8] A similar development occurred in 2020, when a Chinese team reported quantum supremacy using boson sampling.[9] Again, later analysis demonstrated that classical methods could simulate those results more efficiently than initially believed.[10] A follow-up demonstration by Google in December 2024 presented a more refined benchmarking approach, comparing quantum and classical systems on specific tasks.[11] Although not universally accepted as conclusive proof of quantum supremacy, the 2024 results were regarded as significantly more robust and less likely to be overturned by near-term classical improvements. Ongoing evaluation is still required to determine the broader practical implications.

[6] On the choice of the term 'supremacy' here despite its controversial connotations see Preskill, J., 'Why I called it "quantum supremacy"', *Quanta Magazine*, 2 Oct. 2019.

[7] Arute, F. et al., 'Quantum supremacy using a programmable superconducting processor', *Nature*, 24 Oct. 2019.

[8] Pednault, E. et al., 'On "quantum supremacy"', IBM, 22 Oct. 2019.

[9] Zhong, H. et al., 'Quantum computational advantage using photons', *Science*, 3 Dec. 2020.

[10] Oh, C. et al., 'Classical simulation of boson sampling based on graph structure', *Physical Review Letters*, 13 May 2022.

[11] Neven, H., 'Meet Willow, our state-of-the-art quantum chip', Google Quantum AI, 9 Dec. 2024.

Quantum advantage

Closely related but far more practically relevant is the concept of quantum advantage. This is achieved when a quantum computer solves a problem faster or more efficiently than classical methods, with real-world applications—such as in chemistry, optimization or machine learning. Quantum advantage should not be confused with quantum cryptanalysis. The former refers to outperforming classical computers on any useful task, like optimization or simulation, not necessarily decryption.

Nor should quantum advantage be confused with quantum supremacy. Supremacy refers to a demonstration that a quantum device can outperform classical computers on a specific task, even if that task has no practical use. Such tasks are often artificially constructed to be hard for classical systems, such as sampling from complex probability distributions. They are primarily used to showcase the raw computational potential of quantum systems.

Quantum computing today provides no tangible advantage over classical computing in any practical application, whether commercial or scientific. Despite increasing qubit counts and significant investment, current quantum processors have yet to outperform optimized classical algorithms on real-world tasks.[12] At the same time, active efforts to develop robust benchmarking frameworks are under way; for example, recent work presents a systematic overview of component-, system-, software-, and application-level benchmarks, emphasizing that standardized metrics are essential to determine where and when quantum devices might surpass classical machines.[13] Metrics such as quantum volume, circuit layer operations per second (CLOPS) and reliable quantum operations per second (rQOPS) have been proposed to capture scale, speed and reliability, providing concrete criteria to evaluate progress towards quantum advantage. As these benchmarking frameworks mature, they will be key to pinpointing the problem domains and hardware thresholds necessary for a future demonstration of quantum advantage.

Technical challenges and incremental progress

While progress in quantum computing has been rapid, the field remains in an early stage of development. Several key concepts are useful in understanding the technical challenges that it now faces.

1. *Quantum algorithms* refer to step-by-step procedures designed to run on quantum computers. These include algorithms for factoring (e.g. Shor's algorithm), unstructured search (e.g. Grover's algorithm), and linear algebra problems relevant to quantum simulation or machine learning. Quantum algorithms are often compared to classical algorithms, with attention to whether they can solve a problem faster or with fewer resources.

2. *Quantum error correction (QEC)* refers to techniques that protect quantum information from noise and errors. Because individual qubits are fragile, QEC encodes a more stable 'logical qubit'—an error-corrected unit of information built from many physical qubits to ensure reliability over time. This allows computations to continue even when some physical qubits fail.

3. *Noisy intermediate-scale quantum (NISQ)* devices are today's quantum systems, with tens to hundreds of imperfect qubits. These systems are expected to explore useful applications in optimization, materials science

[12] Bobier, J.-F. et al., 'The long-term forecast for quantum computing still looks bright', BCG, 18 July 2024.

[13] Lorenz, J. M. et al., 'Systematic benchmarking of quantum computers: Status and recommendations', arXiv 2503.04905, 6 Mar. 2025.

and quantum chemistry. However, their limited fidelity and qubit count prevent the use of full QEC and limit the size and complexity of the problems they can solve.

Despite recent milestones, quantum computing faces several major challenges.

1. *Scalability and noise*. Current qubits are fragile and error prone. Scaling to useful quantum computers requires thousands or millions of high-fidelity qubits, which is still far from reality.
2. *Logical qubits and quantum error correction*. Implementing effective QEC is essential but resource intensive. Today, protecting a single logical qubit can require hundreds or more physical qubits.
3. *Limited algorithms*. Only a few known quantum algorithms offer clear and provable advantages over classical approaches, and many practical problems still lack efficient quantum solutions—especially for the NISQ devices available in the short term. For example, Grover's algorithm, which is designed to speed up unstructured search tasks, offers only a quadratic improvement in efficiency (i.e. it reduces the number of required steps from n to $\sqrt{n}$), providing a quadratic speed-up over classical approaches. However, for many real-world problems, this increase in speed is not enough to overcome the overheads involved in current quantum hardware and software.[14]
4. *Hardware diversity*. Competing platforms (e.g. neutral atom, photonic, silicon, superconducting and trapped ion) have different characteristics, slowing down standardization and software development.
5. *Verification and benchmarking*. As quantum systems grow in complexity, verifying their results becomes increasingly difficult, especially as systems outpace classical simulators.[15] Verification in quantum computing refers to ensuring that computations are performed correctly and that the outputs are trustworthy. This includes both internal verification (confirming the computation behaved as expected) and external verification (enabling others to check or reproduce results). While small quantum circuits can sometimes be verified using classical simulation, this becomes infeasible at larger scales. Alternative approaches include formal methods, statistical post-processing and interactive protocols for delegated computation. Better tools are needed to benchmark system performance and build confidence in quantum outputs.

Implementing QEC at scale is incredibly demanding. Most schemes—such as the surface code, which arranges physical qubits in a two-dimensional grid to detect and correct errors—require hundreds to thousands of physical qubits to reliably store a single logical qubit. Despite these challenges, real progress has been made: in December 2024 Google reported a major milestone by demonstrating that its error-corrected logical qubit became more reliable as more physical qubits were added—a key indicator that error correction was operating effectively.[16] This result is considered a significant step forward, suggesting that scalable, fault-tolerant quantum computation may be

[14] Hoefler, T., Häner, T. and Troyer, M., 'Disentangling hype from practicality: On realistically achieving quantum advantage', *Communications of the ACM*, vol. 66, no. 5 (May 2023).

[15] Preskill, J., 'Quantum computing in the NISQ era and beyond', *Quantum*, vol. 2 (2018).

[16] Acharya, R. et al., 'Quantum error correction below the surface code threshold', *Nature*, 27 Feb. 2025.

achievable. IBM, meanwhile, has introduced its bivariate bicycle code, which it claims is approximately 10–14 times more efficient than the surface code, potentially offering a more resource-effective path to scalable QEC.[17]

Quantum communications

Quantum communications refer to the use of quantum mechanical principles to develop secure and advanced services for information transfer over quantum networks. As well as relying on such quantum features as superposition and entanglement, these services also rely on the no-cloning theorem, which prevents the copying of unknown quantum states and underpins the security of many quantum protocols.

Quantum networks

A quantum network transmits quantum information—typically using single photons—through optical fibre for short-to-medium distances or free-space links (e.g. satellites) for long-range and global communications. Unlike classical networks, quantum networks require specialized hardware, including single-photon sources and detectors, quantum memory, entanglement generators, and precise timing systems. These components enable the creation, transmission and synchronization of quantum states while preserving coherence by minimizing noise and interference. Quantum networks also rely on classical communications channels to coordinate photon transmission, confirm reception and process outcomes, ensuring reliable operation for tasks such as secure key exchange and entanglement distribution.

While quantum networks provide the physical infrastructure to transmit quantum information—typically encoded in qubits—quantum communications operate at a higher layer, enabling applications like quantum key distribution (QKD), secure clock synchronization, distributed quantum computing and entanglement-based coordination across distant systems. These systems differ fundamentally from classical communications because quantum information cannot be amplified or cloned; it thus requires new architectures such as quantum repeaters, trusted nodes and error-correction mechanisms to scale up across long distances.

For practical purposes, quantum networks are often categorized into two generations based on their capabilities. The first generation, which is already being deployed, allows simple one-way transmission of quantum information, typically using point-to-point links. To cover longer distances, these networks rely on trusted repeaters—intermediate nodes that decrypt and re-encrypt quantum keys before forwarding them. While effective, this approach requires physical trust in every intermediate node and limits the implementation of more advanced quantum protocols. In this generation, the dominant application is QKD, which enables secure key exchange but does not support entanglement-based tasks or distributed quantum computing.

The second generation of quantum networks is more advanced. It enables the distribution of entanglement—that is, the sharing of entangled quantum states between distant nodes in such a way that measurements on one affect the outcome of the other. This forms the foundation for the future quantum internet.[18] Second-generation quantum networks require new components such as quantum repeaters, quantum memories and more sophisticated protocols. With these capabilities, a broader range of services becomes possible—including entanglement-based QKD, distributed quantum computing (where quantum processors at different locations work together on a shared

[17] Yoder, T. J. et al., 'Tour de gross: A modular quantum computer based on bivariate bicycle codes', arXiv 2506.03094, 3 June 2025.

[18] Wehner, S., Elkouss, D. and Hanson, R., 'Quantum internet: A vision for the road ahead', *Science*, 19 Oct. 2018.

task), blind quantum computing (where a user delegates a computation to a quantum server without revealing the input, algorithm or output), precise time transfer (where entangled quantum states are used to synchronize clocks at distant locations with higher accuracy than classical methods), and networked quantum sensing (where spatially separated quantum sensors are entangled to improve sensitivity or resolution beyond what is possible individually). These services open new opportunities for secure communications, coordination and information-processing at a global scale.

Quantum cryptography

The term quantum cryptography is often closely associated with quantum communications as both rely on the principles of quantum physics to enhance security. In most cases, the term refers to QKD, which enables two parties to share securely a secret encryption key that can then be used to protect classical data using standard encryption methods. However, quantum cryptography includes more than just QKD. Other protocols are being developed, such as quantum secure direct communication, where information is transmitted securely without first generating a key, and quantum secret sharing, which allows a message to be split among several recipients and only revealed when they cooperate. These additional tools offer new possibilities for secure communications beyond what is achievable with classical cryptography.

A related component of quantum cryptography is quantum random number generator (QRNG). QRNGs use quantum processes—such as the detection of individual photons or quantum algorithms in quantum computers—to generate random numbers that are fundamentally unpredictable. Unlike classical random number generators, which may rely on deterministic algorithms or physical processes that can be modelled, QRNGs offer a source of randomness that is less susceptible to prediction, making them suitable for cryptographic applications where unpredictability is essential.

Technical and practical challenges

While quantum communications offer unmatched security and future potential, there are also several technical and practical challenges. One of the main limitations is the loss of photons, especially over long distances in optical fibre, which restricts the range of current point-to-point systems. Free-space links (e.g. satellite-based connections) can help extend reach but are weather-dependent and require precise alignment. Most deployed systems today rely on trusted nodes, which are characteristic of the first generation of quantum networks. These nodes reduce end-to-end security if any intermediate node is compromised. Building fully secure, end-to-end quantum networks will require advanced components (e.g. quantum repeaters and quantum memories), which are still in development.

Another key challenge is the certification and verification of QKD systems. Ensuring that the hardware and protocols perform as expected—and are resistant to side-channel attacks—is essential for building trust, especially in sensitive government or military applications.

Finally, integrating quantum networks with existing classical infrastructure—both at the technical and operational levels—remains an open and complex area of development.

Quantum sensing, imaging and metrology

Quantum sensing refers to the use of quantum systems to measure physical quantities such as magnetic fields, electric fields, temperature or acceleration with extremely high sensitivity. These sensors exploit quantum effects such as superposition and entanglement to surpass the performance of classical sensors, particularly in environments

where high precision or weak signals are involved. While the primary advantage is often higher sensitivity or resolution, quantum sensors can also offer benefits in scenarios where they are less precise but significantly smaller, more energy-efficient or better suited for operation in constrained environments. Quantum sensing is typically a passive approach: the quantum system reacts to external physical quantities without actively emitting signals. Examples include quantum magnetometers for detecting submarines or atomic accelerometers for underground navigation without a global navigation satellite system (GNSS) such as the Global Positioning System (GPS).

Quantum imaging is an active process that uses specially prepared light, often involving entangled or squeezed photons (which have reduced quantum noise, allowing more precise measurements), to illuminate an object and detect the returning signal. This enables imaging with higher resolution, better contrast or greater sensitivity under low-light or noisy conditions. Unlike sensing, imaging usually requires a source of quantum light and a detector working together. When classical methods reach their physical limits—for example, imaging through scattering media (e.g. fog or biological tissue) or detecting objects with low reflectivity—quantum imaging is especially valuable. Techniques under development include quantum ghost imaging (which reconstructs an image using correlations between entangled photons, even if the detector has not directly viewed the object) and quantum illumination (which uses quantum correlations to distinguish weak signals from noise, enhancing object detection in cluttered environments).

Quantum metrology uses coherence (i.e. the ability of a quantum system to maintain a well-defined phase relationship, enabling interference) and entanglement to improve precision in measuring time, frequency and other units. One of the most established examples is the optical atomic clock, which uses the precise oscillations of atoms to measure time with extraordinary accuracy—several orders of magnitude beyond the accuracy of current GNSS-based timing systems. Quantum metrology underpins advances in navigation, communications and timing for critical infrastructure.

Despite their promise, quantum sensing, imaging and metrology face several important challenges. Many quantum sensors require highly controlled environments—such as ultra-low temperatures, vacuum chambers or isolation from vibrations—which can limit their use in real-world or mobile settings. One of the key hurdles, especially for military deployment, is meeting size, weight, power and cost (SWaP-C) requirements, a frequently required standard metric for assessing the feasibility of technology integration into operational platforms (e.g. aircraft or submarines). In order to be viable in operational environments, these technologies must be made smaller, lighter, more energy-efficient and cost-effective.

In quantum imaging, challenges include the reliable generation and detection of quantum light, especially under harsh environmental conditions or over long distances. For quantum metrology, maintaining long-term stability and robustness outside laboratory settings remains a significant concern. Across all three areas, moving from laboratory prototypes to rugged, deployable and integrated systems will require advances in materials, engineering and system design. However, recent demonstrations suggest that this transition is already beginning. For example, Q-CTRL's MagNav has shown real-time, GNSS-independent navigation performance that is nearing operational readiness.[19] These early successes highlight that, while hurdles remain, the path to practical quantum sensing in military contexts is actively being developed.

[19] Q-CTRL, 'Q-CTRL overcomes GPS-denial with quantum sensing, achieves quantum advantage', 14 Apr. 2025; and Muradoglu, M. et al., 'Quantum-assured magnetic navigation achieves positioning accuracy better than a strategic-grade INS in airborne and ground-based field trials', arXiv 2504.08167, 10 Apr. 2025.

3. Military and security applications of quantum technologies

Quantum technologies are widely recognized as dual-use, meaning that they can serve both civilian and military applications. Just as the first quantum revolution enabled technologies that transformed both society and modern warfare—such as GPS, lasers and nuclear weapons—today's emerging quantum tools have the potential to reshape future military capabilities. These technologies are being explored across all three major quantum domains: computing, communications and sensing.

Quantum capabilities can enhance military operations across the land, sea, air, space and cyber domains (see figure 3.1). Applications range from secure communications and precise navigation to advanced detection, surveillance and warfare strategies. The range of scenarios also reflects the growing strategic focus and investment from military stakeholders worldwide, who increasingly view quantum technologies as key enablers of next-generation military systems. Before exploring individual examples in detail, it is useful to briefly highlight how each core area of quantum technology contributes to military applications (see box 3.1).[20]

Military and security use cases of quantum technologies

The following use cases demonstrate how emerging quantum technologies are being explored for specific military and security purposes. Each example highlights a distinct area—such as communications, sensing or navigation—in which quantum capabilities may provide strategic advantages or introduce new operational considerations; however, these represent only a fraction of the potential military and security applications under exploration.

Use case: Quantum cryptanalysis and strategic communications security

One of the most significant implications of large-scale universal quantum computing is its potential to compromise widely used encryption methods, especially those based on asymmetric (public-key) cryptography—such as the Rivest–Shamir–Adleman (RSA), elliptic curve cryptography (ECC) and Diffie–Hellman algorithms. These cryptographic systems are used for secure key exchange, digital signatures and authentication in a wide range of applications, including secure email, military logistics systems, critical infrastructure and encrypted government services. While classified communications—whether military, diplomatic or related to national security—typically rely on symmetric encryption (e.g. the Advanced Encryption Standard, AES) for the actual data transmission, public-key systems are still commonly used when two parties first establish a secure connection and for infrastructure-related authentication—this makes them an important part of the overall security architecture. Quantum computing is also expected to reduce the security of symmetric encryption, although to a lesser extent; increasing key lengths can provide adequate protection.[21]

Crucially, the threat is not only in the future. Adversaries may already be employing a so-called harvest-now, decrypt-later strategy—whereby encrypted communications are intercepted and stored today with the aim of decrypting them once powerful quantum computers (also called cryptographically relevant quantum computers, CRQCs)

[20] Krelina, M., 'Quantum technology for military applications', *EPJ Quantum Technology*, vol. 8 (2021).

[21] Barker, E. and Roginsky, A., *Transitioning the Use of Cryptographic Algorithms and Key Lengths*, National Institute of Standards and Technology (NIST) Special Publication no. 800, Initial public draft (NIST: Gaithersburg, MD, Oct. 2024).

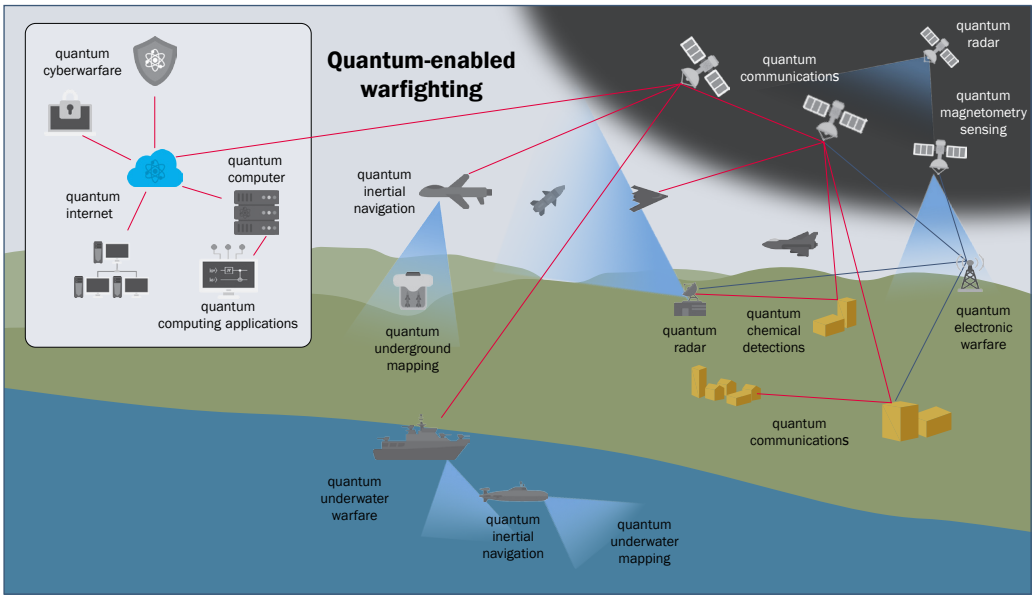


Figure 3.1. Military applications of quantum technologies

This illustration shows a broad range of potential military uses of quantum technologies across various operational domains. It includes applications such as quantum inertial navigation for global navigation satellite system-denied environments: quantum radar and magnetometry for enhanced sensing; quantum communications via satellite for secure links; quantum computing and cyberwarfare capabilities; and underwater and underground mapping using quantum sensors. It reflects how quantum systems could support both strategic command infrastructure and tactical units in the field.

Source: Adapted from Krelina, M., 'Quantum technology for military applications', *EPJ Quantum Technology*, vol. 8 (2021).

become available. This creates a long-term information security risk, especially for sensitive government or military data that must remain confidential for extended periods—often decades.

Estimates vary, but many experts suggest that, depending on technological progress and sustained investment, a CRQC capable of breaking RSA-2048 could emerge within 8–15 years—a moment often referred to as Q-day that will mark the point at which quantum computers can compromise widely used cryptographic systems.[22] This estimate aligns with the most recent assessment by Germany's Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI), which places 15 years as a conservative estimate for the arrival of such a capability.[23] This projected timeline falls within the strategic planning horizon of many military organizations, making quantum-resilient communications a current and strategic priority.

Two main approaches are currently being pursued to mitigate the threat posed by quantum-enabled attacks.

1. *Post-quantum cryptography (PQC)*. PQC focuses on developing new cryptographic algorithms that are believed to resist both classical and quantum attacks. These algorithms are designed to run on today's classical computers and to be deployed in existing digital infrastructure. The US National Institute of Standards and Technology (NIST) is leading a major international effort to standardize PQC algorithms.[24] In 2022 NIST

[22] Mosca, M. and Piani, M., *Quantum Threat Timeline Report 2024* (Global Risk Institute: Toronto, Dec. 2024).

[23] German Federal Office for Information Security (BSI), *Status of Quantum Computer Development*, version 2.1 (BSI: Bonn, Aug. 2024).

[24] US National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC), 'Post-quantum cryptography: Selected algorithms', 12 May 2025.

Box 3.1. Military applications of core quantum technologies

Quantum computing

Quantum computing offers long-term military potential in areas such as cryptanalysis and materials science.[a] In cryptanalysis it may be capable of breaking widely used encryption schemes. In materials science it could enable the simulation and optimization of advanced materials, including stealth coatings and resilient armour. Quantum computing also supports complex optimization tasks, including satellite tasking, mission logistics, coordination of uncrewed aerial vehicles (UAVs) and battlefield navigation. Quantum computing may assist with situational awareness analysis and decision making, and it may power future forms of quantum artificial intelligence (AI). In addition, quantum simulation capabilities are expected to support chemical and biological modelling, including the behaviour of hazardous agents in chemical, biological, radiological and nuclear (CBRN) scenarios.

Quantum communications

Military quantum communications focus mainly on quantum key distribution (QKD), allowing the secure transfer of sensitive information even in contested or surveillance-heavy environments. It also enables precise time transfer and synchronization, which is critical for coordinating radar systems, electronic warfare assets and distributed platforms. In the longer term, quantum networks may support quantum secure direct communication or distributed quantum computing, enabling secure and collaborative computing across distant nodes, which is also useful in coalition operations or cloud-based military infrastructure.

Quantum sensing, imaging and metrology

Quantum sensing and metrology support a wide range of battlefield applications. These include navigation without a global navigation satellite system (GNSS), using quantum inertial navigation, or determining location using the earth's magnetic anomalies or gravity maps. Highly sensitive sensors and clocks can improve radar and electronic warfare systems, either by enhancing detection or improving resistance to jamming. Quantum-enhanced imaging methods can improve intelligence, surveillance and reconnaissance (ISR) capabilities, especially in low-visibility or degraded visual environments.

[a] Śliwa, J. and Wrona, K., 'Quantum computing application opportunities in military scenarios', *2023 International Conference on Military Communications and Information Systems (ICMCIS)* (IEEE: Skopje, 16–17 May 2023).

announced a set of finalists and has since begun preparing final standards; the first three were published in 2024, with additional standards expected by 2025.[25] Many governments and military organizations are already evaluating how to integrate PQC into secure communications systems.

2. *Quantum key distribution.* QKD offers a fundamentally different solution by using the laws of quantum physics to generate and share encryption keys securely. QKD enables the detection of any eavesdropping attempt, making it highly attractive for strategic or high-assurance applications. However, QKD requires specialized hardware and infrastructure, such as quantum communications channels and trusted nodes. It is best suited for specific, high-value links, rather than general-purpose internet traffic.

In practice, PQC is considered the baseline requirement for securing digital communications systems against future quantum threats, given the vast number of digital signatures, keys and secure channels in use across both civilian and military infrastructure. QKD, where technically and operationally feasible, can be layered on top of PQC to provide an additional layer of security for the most sensitive or high-assurance

[25] On Federal Information Processing Standards (FIPS) 203, and 205 see US National Institute of Standards and Technology (NIST), 'NIST releases first 3 finalized post-quantum encryption standards', 13 Aug. 2024.

communications channels—such as those used in strategic command and control or diplomatic messaging. The discussion has never been PQC or QKD; rather, QKD may complement PQC where the highest levels of security are required, while PQC alone will be necessary across the broader digital landscape.

Use case: Quantum communications infrastructure in the European Union and China

The European Quantum Communication Infrastructure (EuroQCI) is a flagship initiative of the EU to build a secure, pan-EU quantum communications network connecting all its member states. Within EuroQCI, the EU Governmental QKD Service (EU-QCI) will focus on enabling QKD for governmental and institutional users.[26] While its initial goal is to provide a highly secure key exchange, the infrastructure may be upgraded to a second-generation quantum network (quantum internet) to support a broader range of quantum communications services, including entanglement-based communications, distributed quantum computing and precise time transfer.

A significant part of EuroQCI is its space segment, known as SpaceQCI, which involves the deployment of quantum communications satellites to enable secure, long-distance links beyond the limits of terrestrial fibre networks. The first demonstrator satellite, Eagle-1, is scheduled for launch in late 2025 or early 2026.[27] It will test satellite-based QKD between space and ground stations in the EU. In parallel, the EU's Nostradamus consortium supports the initiative by establishing a testing and validation laboratory for EuroQCI components, ensuring compliance with security, performance and interoperability requirements.

Beyond its technical objectives, EuroQCI also has strategic significance. It supports the EU's digital sovereignty, reduces reliance on non-EU technologies and strengthens resilience against cyber and quantum-era threats. Notably, 9 of the 26 national EuroQCI projects explicitly reference military-related applications or involve a defence ministry or another military-relevant entity.[28] This reflects a growing awareness of quantum communications as a future enabler of secure command, control and coordination across both civil and military domains in the EU.

In comparison, China has achieved significant strides in quantum communications, establishing the world's largest integrated quantum network. As of early 2025 this network spanned approximately 12 000 kilometres, combining extensive fibre-optic links with satellite-based QKD capabilities.[29] The network includes the Beijing–Shanghai trunk line, a 2000-km fibre-optic QKD link, and has been expanded to link multiple metropolitan areas.

China's quantum communications efforts are bolstered by its space-based segment. The Micius satellite, launched already in 2016, was the world's first quantum communications satellite.[30] It has enabled a number of groundbreaking experiments, including intercontinental QKD between China and Austria. More recently, China demonstrated quantum communications transmission between China and Russia in 2023 and between China and South Africa in 2025.[31] Looking ahead, China plans to expand its quantum

[26] European Commission, Directorate General for Communications Networks, Content and Technology, 'EuroQCI—EU Governmental QKD Service: Concept of operations (ConOps)', version 3.0, 1 Nov. 2024.

[27] European Space Agency (ESA), 'Eagle-1', [n.d.].

[28] European Commission, EU Funding & Tenders Portal, 'EU funded projects', [n.d.].

[29] Groenewegen-Lau, J. and Hmaidi, A., 'China's long view on quantum tech has the US and EU playing catch-up', MERICS China Tech Observatory Quantum Report 2024, Mercator Institute for China Studies (MERICS), Dec. 2024.

[30] Yin, J. et al., 'Satellite-based entanglement distribution over 1200 kilometers', *Science*, 16 June 2017.

[31] Bela, V., 'China and Russia test "hack-proof" quantum communication link for Brics', *South China Morning Post*, 30 Dec. 2023; and Li, Y. et al., 'Microsatellite-based real-time quantum key distribution', *Nature*, 19 Mar. 2025.

satellite constellation, with two to three new quantum communications satellites scheduled for launch into low earth orbit in 2025.[32]

Notably, China's quantum communications infrastructure is closely linked to its national security strategy. Its armed forces, the PLA, are among the primary users of China's quantum communications network, highlighting the technology's dual-use nature and its role in China's civil–military fusion efforts.[33]

Use case: Quantum non-GNSS navigation

Global navigation satellite systems—such as China's BeiDou, the EU's Galileo, Russia's GLONASS and the USA's GPS—have become integral to modern military operations, providing critical positioning, navigation and timing (PNT) services. However, these systems are increasingly vulnerable to jamming and spoofing, especially in contested environments. For instance, in Ukraine, Russian forces have employed electronic warfare tactics that disrupt GPS signals, with an effect not only on military equipment but also on civilian aviation. GPS jamming reportedly affected over 40 000 flights in Eastern Europe over a six-month period, highlighting the scale of this threat.[34]

These vulnerabilities underscore the necessity of alternative means of navigation that do not rely on external signals. Quantum technologies offer a promising path forward, providing accurate and resilient navigation capabilities even in GNSS-denied environments. The leading technologies in this area are quantum inertial navigation and navigation based on magnetic or gravity anomalies.

Quantum inertial navigation. A conventional inertial navigation system (INS) uses accelerometers and gyroscopes to calculate position based on movement from a known starting point. However, such a system accumulates errors over time, leading to drift. Quantum inertial navigation improves on this approach by applying the principles of quantum mechanics, in particular atom interferometry.[35] In this technique, atoms cooled to near absolute zero (i.e. close to –273.15 degrees Celsius or 0 Kelvin) are manipulated with lasers to create interference patterns that can measure acceleration and rotation with exceptional precision. The integration of quantum sensors into navigation systems significantly reduces drift, enabling accurate positioning over extended periods without external references. This capability is particularly valuable for military applications, such as submarine navigation, missile guidance and operations in environments where GNSS access is degraded or denied.

Several programmes are now testing quantum inertial navigation in operational scenarios. A flight trial by the United Kingdom in 2024 marked an early demonstration of GNSS-independent quantum inertial navigation in aviation.[36] Similarly, the United States Naval Research Laboratory is aiming to miniaturize quantum inertial systems for maritime application, although full integration into rugged military platforms remains a key technical hurdle.[37] Moreover, there is significant potential for improvement in terms of SWaP-C. Recent developments, such as a compact quantum rotation sensor

[32] Sharma, A., 'China's strategic ascent in space: New dynamics in 2025', Modern Diplomacy, 22 Jan. 2025.

[33] Qi, C., 'China's quantum ambitions: A multi-decade focus on quantum communications', *Yale Journal of International Affairs*, 2 Feb. 2024.

[34] Poizner, S., 'From Ukraine to Taiwan, jamming of 50-year-old GPS is a defense tech nightmare', Breaking Defense, 22 July 2024.

[35] Travagnin, M., *Cold Atom Interferometry for Inertial Navigation Sensors—Technology Assessment: Space and Defence Applications*, Joint Research Centre (JRC) Technical Report (European Commission: Luxembourg, 2020).

[36] Abdel-Kareem, M., 'UK conducts successful flight trials of un-jammable quantum navigation systems', Quantum Computing Report, 15 May 2024.

[37] Pasquini, N. E. M., 'NRL charters Navy's quantum inertial navigation path to reduce drift', US Naval Research Laboratory, 5 Apr. 2024.

demonstrated in 2024, show progress towards miniaturization and integration of these systems into platforms suitable for military applications.[38]

However, it is important to note that no complete quantum INS has yet been publicly demonstrated. So far, only individual quantum components—either a quantum accelerometer or a quantum gyroscope—have been tested independently in laboratory or early field environments. Integrating these elements into a complete and ruggedized quantum INS suitable for operational deployment remains an open challenge but one that is being actively pursued by military-focused research and development (R&D) programmes.

Navigation based on magnetic and gravity anomalies. Irregularities in the earth's crust cause natural variations in the earth's magnetic field, known as magnetic anomalies. Because these features remain stable over long periods, they provide reliable geophysical reference points for positioning. By comparing locally measured magnetic data with detailed anomaly maps, a military platform (e.g. an aircraft or submarine) can use magnetic anomaly-based navigation to estimate its position, even in the absence of satellite signals.

This approach has recently gained momentum with the emergence of quantum-enhanced magnetic sensors and improved data processing. Notable examples include AQNav, a magnetic navigation solution from SandboxAQ, which combines artificial intelligence (AI) and quantum sensors to provide positioning in GNSS-denied environments.[39] Most recently, in early 2025 Q-CTRL introduced MagNav, a deployable magnetic navigation system that has demonstrated real-time GNSS-independent navigation with performance up to 50 times greater than that of conventional INSs.[40] The advancements reflect that the technology is approaching operational readiness, and it has undergone testing with various military stakeholders in Australia and the USA.[41] Moreover, these examples illustrate the growing importance of integrating AI into quantum sensing applications.

Similarly, navigation based on gravity anomalies uses subtle variations in the earth's gravitational field—caused by irregularities in subsurface mass distributions—as reference points for positioning. By comparing real-time gravity measurements to detailed gravity maps, a platform can determine its location without relying on external signals like GNSS.

Recent advancements in quantum sensing have enhanced the feasibility of this navigation method. For instance, researchers at the University of Birmingham have successfully tested a quantum gravity gradiometer in a maritime environment, demonstrating its potential for mapping and resilient navigation applications.[42] The Jet Propulsion Laboratory of the US National Aeronautics and Space Administration (NASA) is also developing a space-based quantum gravity gradiometer designed to detect gravitational anomalies with increased sensitivity.[43]

The capability to collect, update and access detailed magnetic and gravity anomaly maps is becoming a matter of strategic importance, much like satellite imagery or GNSS control. In both cases, these natural geophysical features can enable reliable, GNSS-independent navigation in environments where satellite signals are unavailable

[38] University of Michigan, 'Proof-of-concept design shrinks quantum rotation sensor to micron scale', Phys.org, 1 Oct. 2024.

[39] SandboxAQ, 'AQNav—AI-based quantum sensing for resilient navigation', [n.d.].

[40] Q-CTRL (note 19); and Muradoglu (note 19).

[41] US Air Force, 'MagNav project successfully demonstrates real-time magnetic navigation', 26 May 2026; and SandboxAQ, 'SandboxAQ completes major AQNav milestones with the USAF', 16 Aug. 2024.

[42] University of Birmingham, 'Quantum sensor for gravity successfully validated at sea', 18 Sep. 2023.

[43] US National Aeronautics and Space Administration, Jet Propulsion Laboratory, 'Nasa aims to fly first quantum sensor for gravity measurements', 15 Apr. 2025.

or compromised—such as under water, in contested airspace or in denied regions. States with advanced mapping capabilities and access to remote or geophysically complex regions will have a distinct operational advantage in deploying these methods effectively. As a result, magnetic and gravity anomaly data sets are emerging as critical resources for security and military operations, with growing relevance for strategic autonomy, precision navigation and operational resilience.

Use case: Quantum radio-frequency receivers

As the electromagnetic spectrum becomes an increasingly contested and vital domain, traditional radio-frequency (RF) systems—used for radar, communications, signal monitoring and spectrum sensing—face growing limitations. Conventional receivers struggle with sensitivity, resilience to signal disruption and size constraints, particularly in dense or denied environments. Quantum RF receivers offer a fundamentally new approach, using quantum properties to detect and analyse RF signals with much greater precision, even under conditions where classical systems may fail. These technologies are particularly applicable to electronic warfare, signals intelligence (SIGINT), communications intelligence, advanced threat detection and radar receiver systems.[44]

Two leading approaches have emerged: one based on Rydberg atoms and another using nitrogen-vacancy (NV) centres in diamonds. Rydberg-based receivers excite atoms to highly sensitive energy states using finely tuned lasers. In these states, the atoms behave like miniature antennas, responding to external RF fields by shifting their internal states and emitting detectable optical signals, which can then be detected. In contrast, NV centres are engineered defects in diamond crystals that respond to RF signals under the influence of magnetic fields, producing changes in fluorescence that can be read optically. Both systems operate at or near room temperature, offer high sensitivity and support broad frequency tunability across the RF spectrum.

What distinguishes quantum RF receivers is their ability to measure the angle of arrival (AOA) of incoming signals with remarkable accuracy—even from sensors placed centimetres apart.[45] Traditional systems require large physical separation between antennas to achieve similar results. This feature enables deployment on satellites, small uncrewed aerial vehicles (UAVs) or other size-limited platforms. Their resistance to jamming, self-calibrating nature and ability to function across wide frequency ranges makes them valuable not just for surveillance, but also for advanced communications, including low-probability-of-intercept and low-probability-of-detection transmissions.[46]

Recent programmes show how quickly the field is advancing. The quantum apertures project of the US Defense Advanced Research Projects Agency (DARPA), led by Honeywell, is developing a programmable, wideband quantum RF receiver that spans frequencies from 10 MHz to 40 GHz and has sensitivity levels far beyond traditional systems.[47] Although most prototypes remain ground-based, efforts are focused on miniaturization and improvements in SWaP-C constraints, paving the way for integration into aircraft, spacecraft or even soldier-carried equipment.

[44] Krelina, M., 'Quantum technologies for air and space (part 2 of 3)—Quantum-enhanced radars and electronic warfare: Use cases and timelines', *Journal of the Joint Air Power Competence Centre*, no. 37 (2024).

[45] Robinson, A. K. et al., 'Determining the angle-of-arrival of a radio-frequency source with a Rydberg atom-based sensor', *Applied Physics Letters*, 15 Mar. 2021.

[46] Fancher, C. T. et al., 'Rydberg atom electric field sensors for communications and sensing', *IEEE Transactions on Quantum Engineering*, vol. 2 (2021).

[47] Uppal, R., 'DARPA quantum apertures (QA) developing employing Rydberg atoms for military electronic warfare, radar, and communications', International Defense Security & Technology, 5 June 2022.

Use case: Quantum magnetometry and chips or brains?

Quantum magnetometry is emerging as a powerful and versatile sensing technology at the intersection of cybersecurity, intelligence and neuroscience. By using quantum effects to detect extremely small magnetic fields, quantum magnetometers are becoming capable of revealing hidden activity from electronic devices—or even neural signals from the human brain. This capability presents both opportunities and challenges. Whether quantum magnetometry becomes a tool for safeguarding critical infrastructure, probing adversary systems or monitoring cognitive states, its dual-use nature suggests that it may serve both defensive and offensive roles in future military and intelligence contexts.

Attacking the chip: Quantum side-channel threats. A side-channel attack (SCA) is a method of extracting sensitive data (e.g. passwords or cryptographic keys), not by breaking the encryption itself, but by exploiting unintended leakages or flaws in a device while it performs cryptographic operations. While classical SCAs typically rely on measuring electromagnetic emissions, acoustic signals, execution timing or power consumption, quantum sensors may take these techniques further. Moreover, because they are more sensitive than conventional tools, quantum devices may detect subtle electromagnetic patterns, fault injections or other microarchitectural vulnerabilities or variations in chip behaviour that are imperceptible to conventional sensors. This could potentially allow adversaries to detect or decode information that was previously considered inaccessible.

The Side-Channel Attacks with Quantum Sensing (SCA-QS) project, launched by Germany's Federal Agency for Innovation in Cybersecurity (Cyberagentur), investigates how quantum sensors could be used to compromise secure microchips.[48] The project aims to test various quantum sensing platforms (e.g. NV-centre diamond sensors and atom-based magnetometers) to evaluate their effectiveness in such attacks and evaluate whether they represent a future threat to secure hardware. This line of research remains at an early stage; however, it highlights a critical trend: advances in quantum sensing may not only enhance defensive capabilities but also open new vectors for attack. Understanding both the opportunities and risks is essential for developing systems that are truly quantum resilient.

Defending the chip: Quantum diamond microscopes. At the same time, quantum magnetometry is also being developed as a defensive tool for microelectronics assurance. In a project led by the Mitre Corporation, researchers developed a quantum diamond microscope (QDM) to detect flaws in microchips used across critical infrastructure, from satellites to aircraft.[49] The QDM uses diamond crystals embedded with NV centres. When placed near an active microchip, these crystals detect the chip's magnetic 'fingerprint', enabling detailed analysis of its internal function.

This tool has two major uses. First, it can identify manufacturing defects, which is especially important as chip components shrink to nanoscale dimensions. Second, it can help uncover malicious modifications, such as hidden logic elements (hardware trojans) inserted during fabrication. Such threats are particularly relevant given the globalized and opaque nature of modern semiconductor supply chains.

Unlike classical microscopes or destructive testing methods, a QDM provides a wide-field, non-invasive means to inspect chips for functional or security-related anomalies.

[48] Cyberagentur, 'Side-Channel Attacks with Quantum Sensing (SCA-QS)', [n.d.].

[49] Lenz, J. N. et al., 'Hardware trojan detection potential and limits with the quantum diamond microscope', arXiv 2402.08004, 12 Feb. 2024.

It can be used alongside other techniques as part of a broader toolkit for supply chain integrity, anti-counterfeit inspection and mission assurance in military systems.

Scanning the brain: Magnetometry and human–machine interfaces. Quantum magnetometry is not limited to microelectronics. One of its most promising—and provocative—applications is in measuring brain activity. Recent advances in wearable quantum sensors, particularly those based on NV centres in diamonds, are enabling brain scanning by magnetoencephalography (MEG) at room temperature.[50] Unlike conventional MEG systems, which are large, expensive, and require cryogenic cooling, quantum magnetometers could lead to portable, high-resolution brain scanners.

These sensors can detect the faint magnetic fields generated by neurons firing in the brain. This opens the door to brain–computer interfaces (BCIs)—systems that interpret brain signals and translate them into digital commands.[51] In military and aerospace contexts, BCIs could enable operators to control UAVs, robots or vehicles with their thoughts, enabling faster decision making and multidomain coordination in complex missions.

Even more speculatively, the ability to scan brain activity discreetly or from a distance raises the possibility of cognitive profiling. In the context of cognitive warfare, such technologies could one day be used to infer emotional states, stress levels or mental intent—supporting psychological operations or decision-shaping efforts. While still theoretical, these ideas are attracting growing attention from military researchers exploring the future of information dominance and human–machine teaming.[52]

Together, these developments show that quantum magnetometry is not limited to one role or one domain. Whether reading the electromagnetic signals of a silicon chip or the brain's own magnetic whispers, this technology offers unprecedented insight into physical and cognitive systems. Depending on how it is used, it could either strengthen the resilience of technologies—or make them more vulnerable to new forms of surveillance and attack.

Quantum + *X*: Integrating quantum with other emerging technologies

In the military context, quantum technologies are unlikely to produce entirely new classes of weapons or military systems on their own. Instead, their strategic impact will come from enhancing and sharpening existing and future military systems—particularly through integration with other emerging and disruptive technologies. This convergence is often referred to as 'quantum + *X*'—where *X* is some other technological domain with which quantum capabilities are combined to deliver significant performance enhancements. NATO has recognized the importance of this paradigm, with ongoing exploration of such areas as quantum + space and quantum + data.[53]

[50] Brookes, M. and Bowtell, R., 'A quantum leap for brain imaging', Vision, University of Nottingham, [n.d.]; and Paek, A. Y. et al., 'Towards a portable magnetoencephalography based brain computer interface with optically-pumped magnetometers', *2020 42nd Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC)* (IEEE: Montreal, 2020).

[51] Liao, K. et al., 'Exploring the intersection of brain–computer interfaces and quantum sensing: A review of research progress and future trends', *Advanced Quantum Technologies*, vol. 7, no. 1 (Jan. 2024); and 'Brain–computer interfaces: Merging human cognition with machines', Quantum Zeitgeist, 29 Sep. 2024.

[52] Binnendijk, A., Marler, T. and Bartels, E., *Brain–Computer Interfaces: US Military Applications and Implications—An Initial Assessment* (Rand Corp.: Santa Monica, CA, 2020).

[53] Reding et al. (note 1).

Quantum + space involves using quantum communications and timing systems for secure satellite links, navigation or space-based situational awareness.[54] Quantum + AI can accelerate machine learning tasks and enhance pattern recognition using quantum sensors and quantum-enhanced optimization. In quantum + autonomy, quantum PNT systems could support GNSS-free operations for autonomous UAVs, submarines or ground vehicles. Other combinations—such as quantum with chemical, biological or even neuroscience-based agents or systems—may support new methods for detection, simulation or protective technologies. Meanwhile, quantum + new materials could enable the development of advanced stealth coatings, sensors or compact energy systems through quantum-enabled materials design.

From a deployment perspective, especially in quantum sensing and metrology, the quantum aspect is often invisible to the end user. Rather than learning new principles, operators simply replace a traditional component—a sensor, a clock, a receiver—with a new 'black box' that offers superior precision, resilience or functionality. This plug-and-play nature makes quantum integration more practical in the near term, as quantum modules can be embedded within existing platforms, infrastructure or command systems with minimal operational disruption.

The power of quantum + *X* lies not in replacing today's systems but in enabling faster, more secure, more autonomous and more capable military operations—across all domains: land, sea, air, space, cyber and cognition.

[54] Krelina, M., 'The prospect of quantum technologies in space for defence and security', *Space Policy*, vol. 65 (Aug. 2023).

4. Quantum and international security

This chapter builds on the analysis of military quantum technologies in chapter 3 by shifting focus from specific applications to their broader implications for international peace and security. While chapter 3 outlines concrete military use cases, this chapter considers how these capabilities could influence deterrence dynamics, arms control regimes and the global security architecture more broadly.

Some commentators have drawn parallels between the strategic importance of quantum technologies and that of nuclear weapons. For example, according to a 2014 article in *China National Defence News*, 'Quantum computing is no less significant than nuclear weapons . . . Once the armies of some countries have quantum computers, while the armies of other countries do not, when a war breaks out, it will be like a blind man fighting with a sighted person. The other party can clearly see what you have, but you cannot see anything.'[55]

The distinct capabilities of quantum technologies, including secure communications, high-precision sensing and advanced computational methods, present both opportunities to enhance resilience and risks that could alter existing security frameworks. On the one hand, they offer new tools for enhancing verification, monitoring and secure communications, potentially supporting more robust arms control frameworks and crisis-management mechanisms. On the other hand, they may challenge existing strategic balances by affecting stealth technologies, weakening or breaking cryptographic systems and introducing asymmetric capabilities. As quantum advances are increasingly integrated into military, intelligence and critical infrastructure systems, governments and analysts are beginning to examine how these technologies may influence deterrence, strategic stability, arms control and geopolitical competition. These dynamics are contributing to increased investments (see box 4.1), the development of new operational concepts, and discussions around the need for coordinated international governance.

This chapter explores how quantum technologies intersect with key pillars of international security, what risks and opportunities they present, and how states are beginning to consider frameworks that support global stability.

Effects on deterrence and strategic stability

Advances in quantum sensing may affect traditional undersea and air-based stealth, with potential implications for nuclear second-strike capabilities. High-precision quantum gravimeters and magnetometers are capable of detecting subtle anomalies in mass or magnetic fields produced by submerged submarines and stealth aircraft. For example, if a state were to deploy quantum sensors capable of tracking deployed nuclear-powered ballistic missile submarines (SSBNs), it could reduce the survivability of these vessels and contribute to crisis instability by making concealed retaliatory forces more vulnerable to early detection and potential pre-emptive targeting (see box 4.2).[56]

While the possibility that quantum sensing could affect second-strike capabilities is increasingly recognized, discussion of its full impact on nuclear stability remains at an early stage.[57] Current analysis focuses primarily on the evolving strategic balance between China and the USA, where both countries are investing in quantum-enabled

[55] Wang, J., [Quantum technology: Changing the face of informational warfare], *China National Defence News*, 8 Jan. 2014 (in Chinese; author translation).

[56] Gamberini, S. J. and Rubin, L., 'Quantum sensing's potential impacts on strategic deterrence and modern warfare', *Orbis*, vol. 65, no. 2 (spring 2021).

[57] Gamberini and Rubin (note 56).

Box 4.1. Government and private investments in quantum technologies

The global quantum technology ecosystem is expanding rapidly, driven by a combination of national security concerns, strategic industrial planning and growing commercial potential. As of mid 2025, governments worldwide have announced US$55.7 billion in public investment dedicated to quantum research and development and infrastructure.[a] These programmes often prioritize sovereign technological capabilities, national security resilience and global competitiveness, especially in the context of great power competition and emerging threats.

In parallel, the private sector is playing an increasingly important role. By April 2024 an estimated $8.5 billion had been invested into quantum technology start-ups, supporting the growth of a dynamic, innovation-oriented industry.[b] This included over 367 active quantum start-ups across computing, communications and sensing. Among these, quantum computing continued to attract the largest share of investment, with approximately $6.7 billion raised by companies working on quantum processors, software and cloud platforms. Quantum communications start-ups had received about $1.2 billion, focusing on quantum key distribution (QKD), secure networking and photonics. In contrast, quantum sensing, while strategically significant and more mature in some areas, had drawn comparatively less attention from investors—receiving only around $700 million.

From a geopolitical standpoint, quantum technologies have become a focus of competition between major powers and strategic groups. Announced government investments highlight how quantum investment aligns with existing strategic groupings and geopolitical rivalries, with China and members of the North Atlantic Treaty Organization (NATO) leading the way (see table).

[a] Qureca, 'Quantum initiatives worldwide 2025', 5 June 2025.
[b] McKinsey & Co., 'Quantum technology monitor', Apr. 2024.

Announced government investments in quantum technologies, mid 2025

State/Group of states	Investment (US$ b.)
Two main global rivals	
China	15.3
United States	7.7
Regional and strategic groups	
EU and partners (Norway, Switzerland)	11.7
BRICS*	17.9**
Indo-Pacific states***	11.6
United States, United Kingdom and Canada	14.2
NATO (cumulative)	24.5

EU = European Union; NATO = North Atlantic Treaty Organization.

* The BRICS group, originally comprising Brazil, Russia, India, China and South Africa, has since expanded into a broader geopolitical coalition that includes Egypt, Ethiopia, Indonesia, Iran and the United Arab Emirates.

** This total includes $15.3 b. from China, $1.83 b. from Russia and $0.72 b. from India.

*** These states are Australia, Japan, South Korea, the Philippines, Singapore, Taiwan, Thailand and New Zealand.

Source: Qureca, 'Quantum initiatives worldwide 2025', 5 June 2025.

detection and counter-detection capabilities. However, the broader literature on how emerging and disruptive technologies—such as hypersonic weapons, cyber operations and AI—might interact with nuclear stability is far more developed than quantum-specific discussions.[58]

[58] Gamberini and Rubin (note 56); Fetter, S. and Sankaran, J., 'Emerging technologies and challenges to nuclear stability', *Journal of Strategic Studies*, vol. 48, no. 2 (Apr. 2025); and Kubiak, K., Mishra, S. and Stacey, G., *Nuclear Weapons Decision-making under Technological Complexity* (European Leadership Network: London, Mar. 2021).

Moreover, outside the relatively balanced China–USA dynamic, there are regions where quantum asymmetries are more pronounced. One example is the relationship between India and Pakistan.[59] India, with its stronger research infrastructure and greater economic resources, is investing in a range of quantum initiatives—from quantum computing projects to QKD pilots.[60] Pakistan, with more limited resources, is progressing more slowly. Such disparities could raise regional security concerns if India's advantages translate into superior surveillance, secure communications or advanced defence capabilities.

Early literature suggested that quantum technologies could either exacerbate crisis instability by reducing the survivability of deterrent forces or, conversely, enhance arms control verification if integrated transparently into monitoring mechanisms.[61] Further focused research will be essential to understand these dual risks and to anticipate how quantum innovations could influence escalation pathways in future conflict scenarios.

A comprehensive assessment of how quantum technologies might reshape strategic stability and deterrence will require the development of conceptual frameworks.[62] More focused technical analyses are urgently needed. Current debates frequently rely on speculative projections, and distinguishing between genuinely emerging capabilities and premature expectations remains difficult, particularly in military and security contexts.[63] For example, quantum technologies may have relevance for operations to counter weapons of mass destruction (WMD), but the maturity and operational viability of such applications require further scrutiny.[64] Without a realistic appraisal of technical feasibility and operational constraints, there is a risk of both overstating hypothetical threats or underpreparing for genuine disruptive shifts. Targeted research focused specifically on military use cases—such as submarine tracking, secure strategic communications, battlefield quantum sensing and chemical, biological, radiological and nuclear (CBRN) detection—can help inform responsible strategic planning and reduce the likelihood of escalation driven by misperceptions or technological misjudgement.

Quantum in C4ISR and information advantage

Quantum technologies are expected to influence future systems for command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) by enhancing security, resilience and data-processing capabilities.[65] Advances in quantum communications, sensing and computing may support new forms of situational awareness that exceed the performance of current systems, potentially offering significant improvements in information processing, threat detection and secure coordination across military and intelligence operations.[66]

[59] Altaf, Z. and Javed, N., 'India's quantum technology advancements: National security implications for Pakistan', *BTTN Journal*, vol. 3, no. 2 (Dec. 2024).

[60] E.g. Indian Ministry of Communications, 'C-DOT and Synergy Quantum sign MOU to jointly develop quantum key distribution technology suited for drone based systems', 12 May 2025; Indian Ministry of Communications, 'C-DOT and Sterlite Technologies Ltd. (STL) achieve India's first quantum key distribution (QKD) over multi-core fibre', 17 Apr. 2025; and Indian Ministry of Defence, 'DRDO & IIT Delhi demonstrate Quantum entanglement-based free-space quantum secure communication over more than 1 km distance', 16 June 2025.

[61] E.g. Doherty, M., 'Quantum technology: The defence imperative', Land Power Forum, Australian Army Research Centre (AARC), 5 May 2020; and Kubiak, K., *Quantum Technology and Submarine Near-invulnerability*, Global Security Policy Brief (European Leadership Network: London, 2020).

[62] Brooksby, A. et al., 'A conceptual framework for describing the future impacts of quantum sensors to national security', *Academia Quantum*, vol. 2, no. 1 (2025).

[63] Biercuk, M. J., 'Read before pontificating on quantum technology', War on the Rocks, 13 July 2020.

[64] Gamberini and Rubin (note 56).

[65] Krelina, M. and Dúbravčík, D., 'Quantum technologies for air and space (part 3 of 3)—Quantum for ISR and PNT: Use cases and timelines', *Journal of the Joint Air Power Competence Centre*, no. 38 (2024).

[66] NATO, 'Summary of NATO's quantum technologies strategy', 17 Jan. 2024.

Box 4.2. A recurring narrative: Quantum and ballistic missile submarines and stealth

A few years ago, a widely circulated narrative suggested that advances in quantum sensing—particularly satellite-borne gravimeters or magnetometers—could soon render the oceans virtually transparent, allowing enemy monitoring of nuclear-powered ballistic missile submarines (SSBNs). Some projections envisioned constellations of space-based quantum sensors triangulating the minute gravitational or magnetic anomalies caused by submerged SSBNs, thereby challenging the survivability that underpins second-strike capabilities.[a]

In practice, however, such orbital quantum sensing will not have sufficient resolution or sensitivity (where these two factors are typically inversely related). Current high-sensitivity quantum sensing systems are still laboratory prototypes or demonstrators mounted on uncrewed aerial vehicles (UAVs). For example, in April 2025 China demonstrated a quantum magnetometer with a sensitivity measured in picoteslas mounted on a UAV—an advance with potential for littoral anti-submarine warfare, but still far from a viable satellite-based capability.[b] Even under ideal conditions, theoretical models suggest that quantum magnetometers operating at their sensitivity limits would enable SSBN detection at ranges up to approximately 10 kilometres. This compares to only a few kilometres for superconducting quantum interference devices (SQUIDs) and several hundred metres for conventional magnetometers.[c]

Meanwhile, China has indicated plans to deploy coastal quantum magnetometer arrays to monitor the South China Sea, aiming to enhance situational awareness through denser sensor networks that address limitations left by conventional magnetic anomaly detection systems.[d] However, even these near-shore installations face constraints related to range, resolution and environmental noise. At the same time, quantum advances in positioning, navigation and timing may help mitigate such threats by enabling SSBNs to operate deeper and longer underwater—beyond the reach of most surface- and air-based sensors. Emerging quantum navigation technologies, including quantum inertial navigation systems (INSs) and quantum magnetic navigation, aim to enable submarines to navigate with high precision without relying on a global navigation satellite system (GNSS). Unlike surface vessels, submarines currently use classical INSs, which suffer from drift over time and typically require periodic synchronization with a GNSS when surfaced; quantum methods could significantly extend underwater navigation autonomy and enhance stealth capabilities (see the use case in chapter 3). At the same time, modern submarine decoys—including autonomous, signature-mimicking gliders and towed arrays—have advanced significantly, further complicating the reliable discrimination of genuine SSBNs from false targets.

This evolution reflects the ongoing dynamic of undersea warfare. As detection technologies improve, so too do techniques for navigation, concealment and deception. For analysts and decision makers, it underscores the importance of assessing both sensor performance and potential counterstrategies in parallel. Without such evaluation, there is a risk of overestimating future detection capabilities or underestimating the resilience of nuclear deterrent forces.

A similar recurring narrative surrounds quantum radar, which is frequently portrayed as a potentially disruptive military technology capable of detecting stealth aircraft. Quantum radar refers to the use of entangled photons or quantum illumination to improve detection of stealth objects. However, experimental findings and technical assessments indicate that quantum radar operating in the radio-frequency domain remains largely impractical with current technology.[e]

[a] Kubiak, K., *Quantum Technology and Submarine Near-invulnerability*, Global Security Policy Brief (European Leadership Network: London, 2020).

[b] Chen, S., 'China unveils drone-mounted quantum device for submarine detection in South China Sea', *South China Morning Post*, 24 Apr. 2025.

[c] Fetter, S. and Sankaran, J., 'Emerging technologies and challenges to nuclear stability', *Journal of Strategic Studies*, vol. 48, no. 2 (Apr. 2025).

[d] Hambling, D., 'China's quantum submarine detector could seal South China Sea', *New Scientist*, 22 Aug. 2017.

[e] Pavan, G., Galati, G. and Daum, F., 'Lessons learnt from the rise and fall of quantum radar research', *Academia Quantum*, vol. 2, no. 1 (2025).

QKD networks and quantum-resistant cryptographic schemes are being developed to protect sensitive command-and-control links from both conventional cyberthreats and future quantum-enabled decryption. A growing number of national and international initiatives recognize the importance of quantum-safe encryption for secure communications infrastructure (see the use case in chapter 3). For example, NATO's Science for Peace and Security programme is already funding pilot projects in quantum-enhanced satellite links and three-dimensional imaging sensors to support secure data exchange across contested or degraded environments.[67]

Next-generation quantum-assured PNT systems—such as quantum inertial navigation and quantum magnetic navigation—are being developed to provide high-precision localization without reliance on GNSS (see the use case in chapter 3). Unlike satellite-based systems, quantum navigation cannot be jammed, spoofed or detected, and it operates passively in all weather conditions and across varied terrain. These features enable missions that were previously limited by inertial drift or the constraints of electromagnetic stealth, expanding operational possibilities in GNSS-denied environments.[68]

Quantum PNT may support autonomous navigation in denied environments, shaping both conventional and unconventional military operations. If realized at scale, such technologies may reduce dependence on space-based infrastructure, improve the survivability of high-value assets, and facilitate the coordination of autonomous and swarming systems. As military concepts evolve towards more decentralized and resilient force structures, assured navigation without external references is likely to become increasingly important for operational flexibility.

Quantum sensing modalities—such as gravimetry and magnetometry—are being explored for their potential to detect, including underground structures, submarines or concealed infrastructure (see box 4.2). These capabilities may affect operational dynamics in domains that have traditionally been reliant on stealth or detection denial. In parallel, advances in quantum computing and quantum machine learning (QML)—a field that applies quantum computing to accelerate pattern recognition and data-classification tasks—could enable more efficient processing of complex, multi-source intelligence data. While still largely experimental, it may offer computational advantages for processing complex intelligence data. Such developments may enhance sensor fusion, target identification and decision making at speeds and scales not currently achievable with classical systems.[69]

Together, these capabilities could contribute to the development of a quantum-enabled C4ISR ecosystem, in which secure communications, resilient navigation and advanced data processing are integrated to improve situational awareness and decision making. However, achieving such integration will depend on coordinated R&D, interoperability standards and rigorous testing—areas currently being explored through various national programmes, international collaborations and military research agencies.

The Q-day cryptographic threat

Large-scale quantum computing could significantly shift intelligence and counter-intelligence. The capacity to break widely used public-key cryptographic systems would compromise the confidentiality of diplomatic communications, military transmissions,

[67] NATO, Science for Peace and Security Programme, *Quantum Technologies and the Science for Peace and Security Programme* (NATO: Brussels, Nov. 2023).

[68] Krelina and Dúbravčík (note 65).

[69] Krelina (note 20).

classified records and critical infrastructure. Unlike many emerging risks, this threat has a well-defined technical foundation: once a quantum computer is powerful enough to run Shor's algorithm at scale, it could decrypt vast stores of intercepted data, including information gathered years earlier under harvest-now, decrypt-later strategies. The future day that this will happen—the point when a quantum computer can break RSA-2048 encryption—is known as Q-day.

What makes this risk particularly complex is the likely uneven pace of quantum progress. Unlike nuclear or space technologies, quantum systems do not necessarily require large-scale physical infrastructure and may advance asymmetrically across states. This raises the prospect of intelligence imbalances, where states that reach Q-day earlier than others could gain covert access to the sensitive communications of less advanced states—including their communications with other, advanced states.

Many developing countries rely on standard encryption to secure government, financial, healthcare, energy and other critical infrastructure systems. Without timely updates to quantum-resilient protections, these systems may become more vulnerable to interception or exploitation by technologically advanced actors. Potential consequences could include unauthorized access to sensitive data, disruption of diplomatic processes, manipulation of domestic political affairs and broader impacts on civilian well-being—raising concerns about a new form of digital asymmetry in the international system.

In this context, the international community—and particularly the United Nations—could play a constructive role. In addition to raising awareness, multilateral organizations may consider supporting capacity-building initiatives to assist their member states in securing critical digital infrastructure. Possible measures include funding for post-quantum cryptography upgrades, technical assistance for system audits, and guidance on managing long-term cryptographic risk. Without early and coordinated efforts, the emergence of quantum-enabled intelligence capabilities could widen global disparities in digital security, leaving some states increasingly exposed to undetectable intrusions or harm to civilians.

Non-state actors and the democratization of quantum technologies

Discussions of quantum technologies in international security have largely centred on state actors, especially military and intelligence agencies. However, as access to quantum tools expands, concerns are growing that non-state actors—including criminal networks, terrorist groups and state-sponsored proxies—could exploit these technologies for malicious purposes.

Although high costs and technical barriers have so far limited non-state access, these constraints are gradually diminishing. Advances in hardware and open-source resources are lowering the entry threshold. The EU Agency for Law Enforcement Cooperation (Europol) has noted that, while the near-term threat is low, it may grow as the technology matures.[70] State-sponsored proxies may be early adopters, potentially using quantum computing for decryption, quantum communications for secure coordination or quantum sensing for surveillance—enhancing their operational capabilities and complicating detection.

Law enforcement bodies such as Europol and the International Criminal Police Organization (Interpol) are beginning to assess quantum-related risks.[71] Europol

[70] Europol, *Do Criminals Dream of Electric Sheep? How Technology Shapes the Future of Crime and Law Enforcement* (Europol: The Hague, 2019).

[71] Europol Innovation Lab, *The Second Quantum Revolution: The Impact of Quantum Computing and Quantum Technologies on Law Enforcement* (Publications Office of the European Union: Luxembourg, 2023).

has called attention to the need for the financial sector to prepare for quantum-era cryptographic threats.[72] Interpol, through its STRATalks Futures Network, warns that advances in quantum computing and quantum communications could further complicate investigations—allowing criminals both to break existing encryption and to adopt inherently secure quantum-encrypted channels.[73]

The democratization of quantum technologies through open-source and open-hardware projects is making basic quantum tools increasingly accessible for education and research.[74] For instance, functional quantum magnetometers have been built for under $150 using off-the-shelf components.[75] While these trends support innovation, they also raise concerns about dual-use risks if malicious actors repurpose such tools.

As accessibility increases, so does the importance of proactive law enforcement engagement, international cooperation and forward-looking regulatory frameworks. Balancing openness with security will be a key challenge as quantum technologies mature.

[72] Europol, *Quantum Safe Financial Forum—A Call to Action* (Publications Office of the European Union: Luxembourg, 2025).

[73] Interpol Innovation Centre, 'STRATalks Futures Network: Interpol global horizon scan', Policing Futures no. 7, Nov. 2021.

[74] Shammah, N. et al., 'Open hardware solutions in quantum technology', *APL Quantum*, vol. 1, no. 1 (Mar. 2024).

[75] Quantum Village, 'Uncut gem', 2025.

5. National and international strategic approaches

Quantum technologies are increasingly recognized not only as drivers of economic and scientific progress but also as strategic assets with major implications for national security. As a result, governments are taking an active role in shaping the development and use of these technologies through dedicated national strategies and international partnerships.

Quantum strategies

Governments are to a greater extent approaching quantum technologies with structured, long-term strategies that reflect national priorities and realistic capabilities. Quantum strategies establish strategic goals and priorities based on a clear analysis of where quantum technologies are headed and how a particular country can position itself for success. These strategies aim to balance support for foundational research, infrastructure development, talent pipelines and industrial competitiveness—recognizing both the extended time horizons involved and the strategic nature of the field.

Not every state will build a full-scale quantum computer or a global quantum communications network. However, some countries have world-leading expertise in quantum algorithms, strengths in quantum sensing or industrial bases that can support specific segments of the quantum technology supply chain (see box 5.1). A well-designed quantum strategy identifies these national advantages, sets focused goals, and ensures that public investment and policy frameworks are targeted to areas where measurable impact is possible. Given that quantum computing poses a serious future threat to cybersecurity—particularly through its potential to break classical encryption—many national strategies also include a dedicated focus on quantum-safe communications and post-quantum cryptography, strengthening defensive capabilities alongside research into potential offensive applications.

The adoption of national quantum strategies has accelerated significantly over the past few years. Between 2017 and 2020 only one strategy per year was launched (see figure 5.1). However, starting in 2021 the number of new national strategies began to rise, with a sharp increase in 2023, when eight countries announced or implemented national quantum initiatives. In 2025 alone, three additional strategies had been recorded by April. This trend reflects the growing recognition among governments that quantum technologies are transitioning from academic research to strategic economic and security domains, requiring clear national planning and coordinated policy action. In some cases, quantum strategies are tied to specific time frames and budgets. For instance, Spain's national quantum strategy, announced in April 2025, outlines investments of €808 million ($922 million) between 2025 and 2030, with the aim of strengthening national capabilities in selected areas of quantum research and innovation.[76]

Quantum strategies are not confined to individual states; they can also be crafted at the multinational level or targeted to specific sectors. For instance, NATO has its own quantum strategy (see box 5.2), and the EU is expected to follow in July 2025.[77] The NATO strategy serves as an example of how multinational coordination can amplify the impact of national efforts. It shows that, while individual states develop their own

[76] Spanish Ministry for Digital Transformation and the Civil Service, 'El gobierno lanza la primera estrategia de tecnologías cuánticas de España con una inversión de 800 millones de euros' [Government launches Spain's first quantum technologies strategy with an investment of 800 million euros], 24 Apr. 2025.

[77] NATO (note 66); and Virkkunen, H., Answer on behalf of the European Commission, European Parliament, 12 Feb. 2025.

Box 5.1. The quantum supply chain

As quantum technologies move closer to practical deployment, attention is increasingly turning to the supply chains that underpin them. Like other advanced technologies, quantum systems rely on a complex ecosystem of specialized components, materials and expertise—including cryogenics, vacuum systems, quantum photonics, superconducting materials, rare earth elements and high-purity lasers. Many of these components are manufactured by a small number of specialized suppliers, often concentrated in specific countries, creating strategic dependencies and potential vulnerabilities.

For military and dual-use quantum technologies, supply chain security is even more critical. Trusted sourcing, intellectual property (IP) control and resilience to geopolitical disruptions are essential to ensure operational reliability and avoid unauthorized transfer of sensitive technologies. This is particularly relevant in the context of growing competition between global powers, where certain components—such as trapped-ion vacuum assemblies or superconducting chip fabrication—may become subject to export controls, restrictions or sanctions.

Recent mapping efforts illustrate how the European Union (EU) remains dependent on non-EU suppliers for such essential components as dilution refrigerators and quantum-specific lasers.[a] The United Nations Institute for Disarmament Research (UNIDIR) is now preparing a framework for assessing vulnerabilities in the quantum supply chain, focused on identifying critical risks, guiding policy action, and supporting resilient and cooperative quantum development.[b] A policy primer on quantum technologies issued by the Organisation for Economic Co-operation and Development (OECD) also highlights the geographic concentration of manufacturing and of ownership of IP, noting that resilience will require both diversification and policy coordination.[c]

A notable example of supply fragility is helium-3 (He-3), an isotope indispensable for reaching sub-Kelvin temperatures in cryogenic systems and neutron detection. He-3 is sourced primarily from nuclear stockpiles—virtually all commercial He-3 originates from the radioactive decay of tritium (H-3), and tritium itself is produced almost exclusively for nuclear-weapon programmes or specialized reactors—and so global availability of He-3 is extremely limited. As demand rises with the growth of quantum sensing and cryogenic quantum computing, shortages or export restrictions could become a significant strategic constraint.[d]

In response, governments are beginning to treat quantum supply chains as critical infrastructure. National initiatives are being launched to map vulnerabilities, incentivize domestic production and integrate supply chain security into funding programmes and procurement standards. For defence and national security applications, this shift is essential—ensuring that future quantum systems are not only technically advanced but also secure, domestically controlled and resilient.

[a] E.g. Mans, U. et al., *Mapping Quantum Supply Chains: Towards European Technology Sovereignty in an Emerging Industry* (Quantum Delta: Delft, [n.d.]).

[b] Cho, D., 'Quantum technologies, global supply chain, and international peace and security', Science, Technology and Security, S. Rajaratnam School of International Studies (RSIS), Apr. 2025.

[c] Barreneche, A., *A Quantum Technologies Policy Primer*, Organisation for Economic Co-operation and Development (OECD) Digital Economy Papers no. 371 (OECD: Paris, Jan. 2025).

[d] Graps, A., 'Helium-3 in the quantum technology supply chain', Quantum Computing Report, 20 Sep. 2024.

quantum road maps based on domestic strengths and priorities, alignment within a broader alliance framework enables resource optimization, standard setting and collective security reinforcement. Similarly, the forthcoming EU strategy is expected to pursue many of the same goals of multinational coordination, supported by access to significant EU-level funding. Together, such multinational strategies are likely to be important for building a coherent and competitive quantum ecosystem that supports both civilian and military applications across allied countries, as well as enabling interoperability, pooled resources and shared standards among member states.

In parallel, sector-specific road maps offer a more focused approach. In the military domain, the Australian Army has published a quantum technology road map

Figure 5.1. Growth in national quantum strategies, 2017–25

The bars show the number of public national quantum strategies launched each year. The figure for 2025 (marked with *) includes strategies announced or initiated up to April 2025.

that identifies priority areas such as quantum sensing for navigation and secure communications.[78] The Canadian Department of National Defence has likewise issued a quantum science and technology strategy implementation plan that details how quantum research will be integrated into procurement and operations over the next decade.[79]

Bilateral and multilateral cooperation

At the bilateral level, the USA has forged a network of formal quantum partnerships framed as joint statements on cooperation in quantum information science and technology. In December 2019 the USA and Japan issued the Tokyo Statement, which sets out core principles—freedom of inquiry, merit-based competition, openness, transparency, accountability and reciprocity—to guide collaborative quantum research.[80] In November 2021 the USA and the UK committed to joint R&D, shared test beds, workforce exchanges and coordinated market-development efforts.[81] By mid 2024 the USA had signed at least 11 such agreements, including with France, South Korea, the Netherlands and several Nordic states, reflecting a broader strategy of aligning allied research programmes and industrial bases.[82]

Other bilateral and multinational arrangements are taking shape. In November 2023 Australia and the UK agreed in a joint statement to share knowledge, align

[78] Australian Army, *Army Quantum Technology Roadmap* (Army Headquarters: Canberra, Apr. 2021).

[79] Canadian Department of National Defence (DND) and Canadian Armed Forces, *Quantum 2030: Quantum Science & Technology Strategy Implementation Plan* (DND: Ottawa, Mar. 2023).

[80] Tokyo Statement on Quantum Cooperation, US Department of State, 19 Dec. 2019.

[81] British–US joint statement on cooperation in quantum information sciences and technologies, Gov.uk, 4 Nov. 2021.

[82] US National Quantum Coordination Office, 'Enhancing competitiveness', [n.d.].

Box 5.2. The North Atlantic Treaty Organization's quantum technologies strategy

The quantum technologies strategy adopted by the North Atlantic Treaty Organization (NATO) in November 2023 includes a classified core document and a publicly available summary.[a] The summary provides an alliance-level framework that complements national and sectoral quantum strategies.

NATO recognizes quantum technologies as strategic dual-use capabilities, with potential applications in sensing, communications, navigation, computing and information science. It also acknowledges the risks associated with technological asymmetry, particularly if adversaries gain superiority in these domains.

The strategy sets out a clear ambition to build a 'quantum-ready Alliance', focusing on coherent investment, interoperability, critical supply chain protection, quantum-safe communications and shared situational awareness across member states. Importantly, NATO emphasizes the need to leverage innovation initiatives such as its Defence Innovation Accelerator for the North Atlantic (DIANA) and the NATO Innovation Fund to accelerate the development and adoption of dual-use quantum technologies, with the goal of enhancing resilience and maintaining a technological edge among NATO forces.

As part of the strategy, in July 2024 NATO launched the Transatlantic Quantum Community, a platform aimed at strengthening collaboration between governments, academia and industry of NATO states.[b] This initiative supports information-sharing, joint research and strategic dialogue on quantum technologies—complementing NATO's strategic objectives with a bottom-up community of practice.

[a] NATO, 'Summary of NATO's quantum technologies strategy', 17 Jan. 2024.
[b] NATO, 'Denmark chairs the inaugural meeting of NATO's Transatlantic Quantum Community', 2 July 2024.

commercialization pathways and strengthen supply chains for quantum technologies.[83] Meanwhile, Australia and India have begun exploring joint quantum projects under the broader Australia–India Comprehensive Strategic Partnership and associated innovation accelerators.[84] These leverage Australia's strengths in photonics and materials and India's expertise in software and system integration. Other examples of bilateral cooperation include India and Italy, France and the Netherlands, and France and Singapore.[85]

At the multilateral level, the EU plays a leading role through such programmes as the Quantum Flagship, Horizon Europe, EuroQCI and the European Defence Fund (EDF). In many cases these require participation from multiple member states to support joint research, co-development of technologies and coordinated deployment of quantum infrastructure across the EU. The stated aim is to strengthen the EU's capabilities in quantum technologies while fostering cross-border collaboration and reducing technological fragmentation.[86]

Other multinational frameworks are also emerging. The trilateral security partnership between Australia, the UK and the USA (AUKUS) identifies quantum technologies as

[83] Australian–British joint statement on cooperation in quantum technologies, Australian Department of Industry Science and Resources, 3 Nov. 2023.

[84] Patil, S., 'The great potential of India–Australia quantum collaboration', The Strategist, Australian Strategic Policy Institute (ASPI), 26 Apr. 2024; and Australian–Indian joint statement on a comprehensive strategic partnership, Australian Department of Foreign Affairs and Trade, 4 June 2020.

[85] Indian Ministry of Science and Technology, 'Italy's minister of university and research Ms Anna Maria Bernini calls on union minister Dr. Jitendra Singh', 11 Apr. 2025; Pollet, M., 'France, Netherlands join forces in quantum technology race', Euractiv, 2 Sep. 2021; and Sharon, A., 'Stronger together: Singapore and France align on emerging tech', OpenGov Asia, 12 Apr. 2025.

[86] European Commission, 'A competitiveness compass for the EU' (note 2).

one of the key pillars for joint development.[87] It places a particular emphasis on secure quantum communications networks and quantum-enhanced navigation systems critical for military operations in contested environments.

The BRICS group, originally comprising Brazil, Russia, India, China and South Africa, has since expanded into a broader geopolitical coalition that includes Egypt, Ethiopia, Indonesia, Iran and the United Arab Emirates (UAE). While BRICS members are increasingly active in the field of quantum technologies, there is currently no formal BRICS-level framework specifically focused on quantum technologies.[88] However, there are several important bilateral initiatives among BRICS members in the quantum domain. China and Russia have jointly tested a secure quantum communications link, demonstrating a possible model for quantum-secure data exchange between strategic partners.[89] China and South Africa have collaborated on establishing a quantum satellite link, with public claims that China intends to use its quantum satellite capabilities to support secure communications across the broader BRICS group.[90] Similarly, India and Russia have initiated cooperation on quantum technologies, exploring areas such as trapped-ion-based quantum computing and quantum sensing.[91] These emerging collaborations indicate that major emerging economies are beginning to pool resources and expertise in quantum research, with the potential to enhance regional security cooperation and support technological development.

[87] Luckenbaugh, J., 'AUKUS countries team up to develop key quantum capabilities', *National Defense*, 17 Feb. 2023.

[88] Survé, I. and Mdlokovana, S., 'BRICS bloc quantum computing race: Breaking the Western tech monopoly', IOL, 14 Mar. 2025.

[89] Bela (note 31).

[90] Bela, V., 'China creates hacker-proof quantum communication link with South Africa', *South China Morning Post*, 13 Mar. 2025.

[91] 'Russia, India explore prospects for cooperation in quantum technologies', TASS, 9 July 2024.

6. National and multilateral governance of and through quantum

Building on their strategic priorities, governments are now implementing concrete governance measures to steer the quantum landscape. These approaches extend beyond funding and research support to include regulatory tools such as export controls, technical standards and early-stage arms control discussions. Together, these mechanisms reflect an evolving effort to balance innovation with security, and openness with control. This chapter explores the key tools states are using to guide quantum development and mitigate emerging risks.

Export controls and research security

As quantum technologies advance towards real-world deployment, governments are increasingly focused on controlling their spread and strategic use. Export controls, investment restrictions, visa policies and international agreements are becoming critical tools for managing the global flow of quantum expertise, components and systems. These measures can serve a variety of functions, including protecting national and international security, supporting international law and human rights, and preventing adversaries from accessing potentially disruptive capabilities.

A key multilateral framework in this area is the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-use Goods and Technologies. The Wassenaar Arrangement's lists of military items and dual-use goods and technologies potentially captures a range of quantum technologies, including certain quantum sensors and quantum computers and their related components.[92] Because the Wassenaar Arrangement and similar multilateral regimes are structured around the capabilities of items (e.g. high-precision sensors, stealth materials, advanced computing), they already encompass quantum-enhanced devices in those categories—no separate catch-all for 'quantum technologies' is needed to cover a quantum technology-powered sensor or quantum technology-derived stealth system. In recent years, the 42 participating states have updated the Wassenaar Arrangement's dual-use list to cover quantum cryptography systems and post-quantum cryptography. However, recent efforts to adopt new controls on quantum technologies have been politically challenged.[93] Notably, reflecting broader geopolitical tensions, in late 2023 Russia blocked proposals to update the Wassenaar Arrangement's control lists to add quantum computers and related subcomponents.[94] As a result, many states have moved forward with national-level controls. For example, the UK has amended its Export Control Order to include quantum computing, cryogenic technologies and specialized quantum sensing equipment within its list of strategic goods requiring a licence for export.[95] The UK has noted that coordination among NATO members and close partners like Australia under the AUKUS agreement supports the UK's efforts to align controls on sensitive quantum

[92] Wassenaar Arrangement Secretariat, *Public Documents*, vol. II, *List of Dual-use Goods and Technologies and Munitions List* (Wassenaar Arrangement: Vienna, 2024); and European Commission, 'Emerging technologies developments in the context of dual-use export controls', Fact sheets, Nov. 2020.

[93] Benson, E. and Mouradian, C., *Establishing a New Multilateral Export Control Regime* (Center for Strategic and International Studies: Washington, DC, Nov. 2023).

[94] Stewart, I. J., 'Are new US export controls rules on chips and other critical tech good enough?', *Bulletin of the Atomic Scientists*, 13 Sep. 2024; and Bromley, M. et al., 'Dual-use and arms trade controls', *SIPRI Yearbook 2025: Armaments, Disarmament and International Security* (Oxford University Press: Oxford, 2025).

[95] Export Control (Amendment) Regulations 2024, British Statutory Instrument no. 2024/346, 7 Mar. 2024.

technologies.[96] However, the lack of agreement at the Wassenaar level and the resulting patchwork approach have created uncertainties for companies and researchers working internationally. Sections of the global research and industrial community have complained that these new controls have been adopted without fully disclosing their rationale, raising concerns about their potential impact.[97]

The USA has taken significant steps to tighten its quantum export regime and used it to try to limit the supply of key components and technologies to China. Under the Export Administration Regulations (EAR), the US Department of Commerce has added restrictions on the export of key quantum computing equipment, materials and software.[98] At the same time, the US Department of the Treasury introduced investment bans aimed at limiting the flow of US capital into China's quantum technology sector.[99] These specifically target areas where quantum capabilities could enhance China's military and intelligence potential. Additionally, inbound investments into sensitive US quantum companies are closely scrutinized for national security risks by the Committee on Foreign Investment in the United States (CFIUS).[100]

China, for its part, has reinforced its own controls through its Export Control Law and new regulations effective from late 2024.[101] These measures require licensing for the export of quantum computers, communications hardware, cryogenics and related subsystems, particularly where dual-use or military applications are involved. In parallel, new restrictions and administrative hurdles are making international collaboration more difficult in sensitive areas of quantum research.[102] These developments align with China's broader efforts to strengthen domestic control over strategic technologies and reflect national priorities in security and technological self-reliance.

India's system of dual-use export controls is based on the Special Chemicals, Organisms, Materials, Equipment and Technologies (SCOMET) list.[103] This draws from multilateral frameworks such as the Wassenaar Arrangement, in which India participates.

The EU updated its export control framework through the 2021 recast of the Dual-use Regulation.[104] Among other changes, the recast gave each EU member state the ability to regulate exports from its territory using the national control list of another EU member state—referred to as 'transmissible controls'—including in relation to emerging technologies. The coverage of the Dual-use Regulation is outlined in the EU dual-use list, which integrates the Wassenaar dual-use list and the control lists of the other multilateral export control regimes. The EU and EU member states have been discussing the creation of an autonomous EU dual-use list that would include items that all member states would like the multilateral regimes to adopt but that have been

[96] British Ministry of Defence, 'Historic breakthrough in defence trade between AUKUS partners', Press release, 15 Aug. 2024.

[97] Sparkes, M., 'Multiple nations enact mysterious export controls on quantum computers', *New Scientist*, 3 July 2024.

[98] US National Quantum Coordination Office, 'Department of Commerce releases export controls on quantum technologies', 6 Sep. 2024.

[99] US Department of the Treasury, 'Treasury issues regulations to implement executive order addressing US investments in certain national security technologies and products in countries of concern', 28 Oct. 2024.

[100] Plotinsky, D. and Hilferty, K. M., 'Current technology risks assessed by US government regulatory tools', Morgan Lewis, 30 June 2023.

[101] Xu, R. et al., 'Final version of China's Export Control Law will take effect in less than two months', Hogan Lovells, 23 Oct. 2020; and Sheng, J. and Xu, C., 'China issues new export control regulations on civil–military dual-use items', Pillsbury Law, 7 Nov. 2024.

[102] Matthews, D., 'Chinese export rules make collaboration riskier, researchers warned', Science Business, 29 Aug. 2024.

[103] Indian Ministry of External Affairs, 'India's strategic trade controls and SCOMET list', [n.d.].

[104] Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast), *Official Journal of the European Union*, L 206, 11 June 2021.

blocked (e.g. the proposed Wassenaar Arrangement controls on quantum computers); however, this list has not yet been established.[105] The Dual-use Regulation includes a set of catch-all controls that member states can use to regulate exports of items that are not covered by the EU dual-use list—including exports of quantum systems—but these only apply in specific cases (e.g. military end use in embargoed destinations or for WMD purposes).

In early 2025 the European Commission called on EU member states to initiate mechanisms for screening outbound investment that focus on critical technologies, including quantum, semiconductors and AI.[106] This step aims to assess potential risks to economic and national security through the decision-making authority that remains with individual member states.

Hand in hand with traditional export controls—which regulate not only physical items and software but also 'technology' in the export control sense (i.e. the technical data and technical assistance required for the development, production or use of controlled items)—a growing number of states, including EU member states and the USA, have shown an interest in strengthening research security, particularly in such sensitive fields as quantum technologies. Research security focuses on protecting knowledge, expertise and innovations emerging from universities and research centres from undesirable transfer, espionage and misuse. This includes guarding against risks such as sharing sensitive designs through academic collaborations, technical publications or international conferences. For example, a 2024 EU recommendation on research security highlights that existing export control rules already cover transfers of intangible technology (i.e. technical data and assistance) and urges universities and laboratories to recognize and comply with these requirements as part of their security processes.[107] It calls for greater awareness within academia and encourages better coordination between research institutions and national authorities to help mitigate proliferation risks at an early stage.

As part of this broader landscape, some countries are also integrating counterintelligence efforts into their quantum research protection strategies. In the USA, for instance, the National Counterintelligence Task Force has established a Quantum Information Science Counterintelligence Protection Team (QISCPT) to address espionage and foreign influence operations targeting sensitive quantum research.[108] This team, which brings together agencies including the Federal Bureau of Investigation (FBI), works with universities, laboratories and companies to raise awareness, provide tailored risk briefings and support the implementation of security protocols.

To complement this targeted research security, policymakers are also reassessing the broader fit of existing arms control regimes. Although multilateral export controls already capture quantum-enhanced capabilities and intangible technology transfers, governments and research institutions continue to find it difficult to even identify which quantum knowledge flows fall under these rules. As a result, complementary research security initiatives—such as tailored outreach programmes, risk-assessment briefings and counterintelligence-support teams—have been deployed to ensure that universities, laboratories and industry partners recognize their export control obligations and put effective compliance processes in place.

[105] Bromley et al. (note 94).

[106] European Commission, 'Commission calls on member states to review outbound investments and assess risks to economic security', Press release, 15 Jan. 2025.

[107] Council of the European Union, Council recommendation of 23 May 2024 on enhancing research security, *Official Journal of the European Union* C, 30 May 2024; and Héau, L., 'The EU research security initiative: Implications for the application of export controls in academia and research institutes', Non-proliferation and Disarmament Papers no. 94, EU Non-proliferation and Disarmament Consortium, Mar. 2025.

[108] US Federal Bureau of Investigation (FBI), 'Protecting quantum science and technology', 12 Apr. 2024.

These developments reflect a growing trend: quantum technologies are increasingly treated not only as scientific assets, but also as strategic targets—prompting both export control regimes and counterintelligence frameworks to evolve in parallel. This has caused governments to adapt traditional counterintelligence frameworks to emerging technological domains.

Other regulations

Participation limits

Beyond export controls and strategic partnerships, a range of sector- and project-specific rules define who can participate in quantum programmes and under what conditions. For example, the EDF restricts funding eligibility to organizations established in the EU and owned or controlled by EU member states.[109] Similarly, Horizon Europe (the EU's framework programme for research and innovation) limits participation to legal entities in the EU or its associated countries (e.g. Canada, Israel, Norway).[110] In 2025 Switzerland and the UK, which had been excluded from sensitive or strategic calls (including those in quantum and space technologies), regained access to these strategic areas, expanding opportunities for participation in critical research domains.[111]

In China, foreign firms encounter multiple layers of regulation. In many cases, before an overseas technology company can operate in a strategic sector, the company is required by the Foreign Investment Law and the accompanying Negative List to form a joint venture with a domestic partner—often involving partial ownership or licensing of intellectual property rights.[112] Projects tied to security protection of critical information infrastructure (which includes quantum communications networks) require government approval and typically necessitate a domestic majority stake for enterprises operating in areas with national security implications.[113]

Navigating dual-use research

Dual-use is a key regulatory dimension. The dual-use nature of quantum technologies means that they can serve both civilian and military ends, often with little or no modification. For example, a quantum sensor developed for geological surveys could also be used to detect submarines; a quantum communications link built for financial data security could support classified military communications. This dual-use character presents both opportunities and challenges: it enables innovation through commercial investment and research, but it also raises concerns related to technology control, export restrictions, proliferation risks and the need for strategic oversight. Governments and international bodies will need to balance support for open scientific progress with safeguards to prevent misuse or unintended technological advantage by potential adversaries.

For example, within EU funding programmes, projects with direct military applications were explicitly excluded from the original Horizon Europe. In March 2024,

[109] Regulation (EU) 2021/697 of the European Parliament and of the Council of 29 April 2021 establishing the European Defence Fund, *Official Journal of the European Union*, L 170, 12 May 2021.

[110] Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe, *Official Journal of the European Union*, L 170, 12 May 2021.

[111] Greenacre, M. and Matthews, D., 'UK and Switzerland to gain access to "strategic" Horizon Europe calls', Science Business, 30 Apr. 2025.

[112] Foreign Investment Law of the People's Republic of China, promulgated by Presidential Order no. 26, 15 Mar. 2019; and Chinese National Development and Reform Commission and Chinese Ministry of Commerce, 'Special Administrative Measures (Negative List) for Foreign Investment Access (2024 edition)', 8 Sep. 2024.

[113] Critical Information Infrastructure Security Protection Regulations, promulgated by Chinese State Council Order no. 745, 30 July 2021.

however, the European Commission announced that certain calls would be opened to dual-use and military-relevant topics, provided that they undergo stricter ethical, legal and security reviews to safeguard sensitive knowledge and technologies.[114]

At the national level, Germany provides a notable example of evolving policy. Historically, many German universities chose not to engage in dual-use research or cooperation with the German armed forces (the Bundeswehr), reflecting a strong post-World War II culture of civilian control. However, following Russia's 2022 full-scale invasion of Ukraine, these restrictions have been reassessed. The 2025 post-election agreement between the new governmental coalition parties commits to 'expand peace and conflict studies and regional research (e.g. on Eastern Europe, China and the USA) and establish a funding framework for security and defence research—including cybersecurity and resilient infrastructures—to enable more targeted cooperation of universities and non-university research institutions with the Bundeswehr and industry'.[115] Furthermore, it explicitly states: 'We are committed to removing obstacles that, for example, impede dual-use research or civil–military research cooperation.'[116] Germany also aims to strengthen research security by developing guidelines for sensitive international contexts, building advisory infrastructures and establishing expert commissions to 'de-risk' relations with strategic partners such as China.

This set of measures illustrates how national policy is being adapted in response to geopolitical developments, embedding dual-use quantum research within a broader strategy of resilience, security and strategic autonomy.

Quantum and ethics

Alongside legal regimes, a growing landscape of research ethics initiatives has emerged. The Centre for Quantum and Society in the Netherlands, the Innsbruck Quantum Ethics Lab in Austria, the Quantum Social Lab in Munich, Germany, and the Quantum Ethics Project in the USA each examines the societal impacts of quantum technologies. In 2025 a community-driven call was published encouraging the development of comprehensive ethics frameworks for quantum research, although it primarily addresses broader societal and ethical issues and pays limited attention to areas such as international security, dual-use risks or strategic competition.[117]

Unfortunately, few of these centres explicitly address the international security dimensions of quantum—such as espionage, dual-use proliferation or strategic weaponization. A good example of an exception is a call made in 2024 for new ethical governance frameworks focused on military-related applications.[118] This gap highlights the need for a dedicated laboratory or centre to analyse and inform the geopolitical and security implications of quantum technologies, helping ensure that ethical oversight evolves in step with both technological development and emerging strategic risks.

[114] European Commission, High Representative of the Union for Foreign Affairs and Security Policy, 'Joint white paper for European defence readiness 2030', JOIN(2025) 120 final, 19 Mar. 2025; and European Commission, 'Proposal for a regulation of the European Parliament and of the Council amending Regulations (EU) 2021/694, (EU) 2021/695, (EU) 2021/697, (EU) 2021/1153, (EU) 2023/1525 and 2024/795, as regards incentivising defence-related investments in the EU budget to implement the ReArm Europe Plan', COM(2025) 188 final, 22 Apr. 2025.

[115] German Christian Democratic Union (CDU), Christian Social Union (CSU) and Social Democratic Party (SPD), 'Verantwortung für Deutschland' [Responsibility for Germany], Coalition agreement, 9 Apr. 2025, p. 79 (author translation).

[116] German Christian Democratic Union et al. (note 115), p. 131 (author translation).

[117] Vermaas, P. E. et al., 'Societal research for quantum technologies: A vision for Europe', Zenodo, Jan. 2025.

[118] Taddeo, M., Blanchard, A. and Pundyk, K., 'Consider the ethical impacts of quantum technologies in defence—Before it's too late', *Nature*, 24 Oct. 2024.

Arms control, arms verification and confidence-building

Quantum technologies may offer novel tools with potential applications in arms control verification. Quantum sensors—such as gravimeters, magnetometers and satellite-based QKD receivers—could eventually enable remote monitoring capabilities sensitive enough to detect clandestine nuclear tests or treaty-limited activities from space, potentially enhancing arms control efforts beyond the reach of current systems.[119] Similarly, quantum communications links could be used to secure treaty-related data exchanges, helping to protect the integrity and confidentiality of verification information.

However, integrating quantum capabilities into verification regimes is likely to require new confidence-building measures (CBMs). Drawing on recent AI proposals, states could adopt reciprocal sensor data-sharing, joint quantum-sensor field trials, and transparent calibration and cross-validation procedures.[120] These steps would reduce uncertainty about sensor performance and foster trust without raising fears of unauthorized surveillance.

Before integration, comprehensive assessments are needed that move beyond speculative discussions. Research should evaluate how quantum sensing technologies (e.g. gravimetry, magnetometry, spectroscopy and single-photon detection) can enhance arms control and verification, including their fidelity and advantages over existing methods. A November 2024 workshop recommended exploring quantum tools for verifying nuclear and chemical weapons, but systematic comparisons of traditional versus quantum-enhanced approaches in specific contexts remain scarce and warrant further study.[121]

Looking ahead, it would be helpful to assess where quantum technologies could fit into current and future verification frameworks. As quantum technologies advance, international bodies might consider them in review conferences for international treaties, such as the 1972 Biological and Toxin Weapons Convention (BWC) and the 1993 Chemical Weapons Convention (CWC), to address resulting challenges and opportunities.[122] New governance models could be explored that would aim to manage research transparency or monitor offensive quantum-enabled capabilities. For example, the Scientific Advisory Board of the Organisation for the Prohibition of Chemical Weapons (OPCW) could inspire the incorporation of scientific expertise into treaty governance.[123] Furthermore, since quantum computing may speed up tasks such as protein folding—useful for drug discovery but also for bioengineering threats—the dual-use nature of quantum-enabled breakthroughs will need greater attention in regulatory and ethical frameworks.[124]

[119] Malekos Smith, Z. L. and Persi Paoli, G., *Quantum Technology, Peace and Security: A Primer* (United Nations Institute for Disarmament Research, UNIDIR: Geneva, 2024).

[120] Malekos Smith and Persi Paoli (note 119).

[121] SIPRI and Quantum Delta Netherlands, Expert workshop on arms control implications of quantum technologies, The Hague, 22 Nov. 2024; and SIPRI, 'SIPRI researchers lead discussions on quantum technologies', 17 Dec. 2024.

[122] Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction (Biological and Toxin Weapons Convention, BWC), opened for signature 10 Apr. 1972, entered into force 26 Mar. 1975; and Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (Chemical Weapons Convention, CWC), opened for signature 13 Jan. 1993, entered into force 29 Apr. 1997.

[123] Krelina, M., 'An introduction to military quantum technology for policymakers', SIPRI Background Paper, Mar. 2025.

[124] Doga, H. et al., 'A perspective on protein structure prediction using quantum computers', *Journal of Chemical Theory and Computation*, vol. 20, no. 9 (14 May 2024).

Cybersecurity and quantum resilience

In the realm of cybersecurity and quantum resilience, governments worldwide are racing to adopt post-quantum cryptography—cryptographic algorithms believed to resist attacks by both quantum and classical computers.

In the USA, NIST has completed its first round of PQC standardization, publishing three key algorithms in August 2024 and encouraging system administrators to begin the transition to PQC immediately.[125] NIST has drafted a road map for agencies to transition from quantum-vulnerable schemes, with legacy algorithms such as RSA, ECC and Diffie–Hellman scheduled for deprecation by 2030 and full disallowance by 2035.[126] Meanwhile, international standards bodies are working to ensure global consistency. A joint technical committee of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), through a working group on cryptographic techniques, is preparing an amendment to the widely used ISO/IEC 18033-2 standard for information technology (IT) security techniques and encryption algorithms.[127] This amendment will integrate post-quantum algorithms into the standard international cryptographic suite, helping to ensure that global systems adopt consistent and quantum-resilient encryption methods.

In the UK, the National Cyber Security Centre (NCSC) has issued a three-phase timeline: complete an enterprise-wide cryptographic 'discovery' by 2028; execute high-priority PQC migrations by 2031; and finish full deployment by 2035.[128]

Within the EU, the European Commission has called on member states to develop harmonized strategies for transitioning to PQC. In April 2024 it issued a formal recommendation to states to define clear goals, milestones and hybrid (PQC and classical) schemes by 2026.[129] However, cryptographic algorithm selection and mandatory security standards remain national competencies within the EU; the Commission can only issue recommendations and cannot impose binding requirements. As a result, national guidance across the EU varies. For example, France's National Agency for the Security of Information Systems (Agence nationale de la sécurité des systèmes d'information, ANSSI) recommends a phased adoption of PQC beginning immediately and continuing until 2030, with a preference for hybrid cryptographic schemes.[130] Germany's BSI also supports the use of hybrid schemes, but its recommended selection of algorithms partly differs from the French approach.[131] In contrast, Czechia's National Cyber and Information Security Agency (Národní úřad pro kybernetickou a informační bezpečnost, NÚKIB) endorses the use of pure post-quantum algorithms in certain cases and has set a national goal of achieving PQC readiness by 2027 for sensitive information of a critical level of confidentiality in a risk environment.[132] At the

[125] US National Institute of Standards and Technology (note 25).

[126] Moody, D. et al., *Transition to Post-quantum Cryptography Standards*, Initial public draft, National Institute of Standards and Technology (NIST) Internal Report no. 8547 (NIST: Gaithersburg, MD, Nov. 2024).

[127] Moody, D., 'NIST post-quantum cryptography update', US National Institute of Standards and Technology (NIST), 2023.

[128] British National Cyber Security Centre (NCSC), 'Timelines for migration to post-quantum cryptography', 20 Mar. 2025.

[129] Commission Recommendation (EU) 2024/1101 of 11 April 2024 on a coordinated implementation roadmap for the transition to post-quantum cryptography, *Official Journal of the European Union* L, 12 Apr. 2024.

[130] French National Agency for the Security of Information Systems (ANSSI), 'ANSSI views on the post-quantum cryptography transition (2023 follow up)', 29 Aug. 2023.

[131] German Federal Office for Information Security (BSI), *Cryptographic Mechanisms: Recommendations and Key Lengths*, BSI Technical Guideline TR-02102-1, version 2025-01 (BSI: Bonn, 31 Jan. 2025).

[132] Czech National Cyber and Information Security Agency (NÚKIB), 'Minimální požadavky na kryptografické algoritmy: Doporučení v oblasti kryptografických prostředků' [Minimum requirements for cryptographic algorithms: Recommendations on cryptographic resources], version 4.0, 5 Feb. 2025; and NÚKIB, 'Kvantová hrozba a kvantově odolná kryptografie—Příloha k dokumentu: Minimální požadavky na kryptografické algoritmy'

EU level, efforts to coordinate implementation have continued. In April 2025 the EU Agency for Cybersecurity (ENISA) released an updated catalogue of state-of-the-art classical and post-quantum algorithms, offering practical guidance and highlighting common implementation pitfalls.[133] This was followed in June 2025 by a new European Commission road map that builds on the 2024 recommendation, calling for member states to finalize national PQC plans by 2026 and complete phased implementation by 2035 with significant milestones in 2030.[134]

China has launched a PQC programme under the Institute of Commercial Cryptography Standards, soliciting candidate algorithms for national standardization.[135] This reflects concerns about external dependencies and the perceived risk of 'back doors' in foreign-developed schemes. Among other countries also advancing their efforts, Japan has its Cryptography Research and Evaluation Committees (CRYPTREC); South Korea's Ministry of Science and Information and Communications Technology (MSIT) has a road map targeting completion by 2035; and the Monetary Authority of Singapore (MAS) has issued guidance for PQC planning in the financial sector.[136]

As PQC moves from research to deployment, these overlapping standards, timelines and national strategies highlight the growing need for sustained coordination—both regionally (e.g. within the EU) and globally—to ensure the resilience of critical infrastructure against future quantum-enabled threats.

Quantum standardization

As quantum technologies mature, international standardization is becoming increasingly important to ensure interoperability, security and widespread adoption. Key international standards bodies have launched initiatives to define fundamental terminology, technical protocols and security requirements. In September 2019 the International Telecommunication Union (ITU) established the Focus Group on Quantum Information Technology for Networks (FG-QIT4N) under its Telecommunication Standardization Sector (ITU-T).[137] A series of pre-standardization technical reports—including the definition of use cases, protocols and reference architectures for quantum communication networks—issued by the focus group that laid the groundwork for future ITU-T recommendations.

Similarly, the ISO and IEC are also active, particularly through a standardization subcommittee on information security, cybersecurity and privacy protection of their joint technical committee (JTC) on IT (ISO/IEC JTC 1/SC 27).[138] In addition to working on the integration of PQC into global security standards, a dedicated standard (ISO/IEC 23837-1:2023) published in 2023 outlines general security requirements for QKD

[Quantum threat and quantum resistant cryptography—Annex to the document 'Minimum requirements for cryptographic algorithms'], version 2.0, 5 Feb. 2025.

[133] European Cybersecurity Certification Group, Sub-group on Cryptography, 'Agreed cryptographic mechanisms', version 2.0, EU Agency for Cybersecurity (ENISA), Apr. 2025.

[134] European Commission, Network and Information Systems (NIS) Cooperation Group, *A Coordinated Implementation Roadmap for the Transition to Post-quantum Cryptography*, part 1, version 1.1, EU PQC Workstream (European Commission: Brussels, 11 June 2025).

[135] Agarwal, A., 'China's quantum strategy: Launching quantum-resistant encryption standards and protecting data from emerging threats', GrackerAI, 18 Feb. 2025.

[136] GSM Association (GSMA), 'Post quantum cryptography—Guidelines for telecom use cases', version 1.0, 22 Feb. 2024.

[137] International Telecommunication Union (ITU), 'ITU-T Focus Group on Quantum Information Technology for Networks (FG-QIT4N)', 2021.

[138] International Organization for Standardization (ISO), 'ISO/IEC JTC 1/SC 27: Information security, cybersecurity and privacy protection', [n.d.].

systems.[139] This standard defines essential security characteristics intended to support the robustness and trustworthiness of quantum communications systems. Meanwhile, the Institute of Electrical and Electronics Engineers (IEEE) Quantum Initiative coordinates several working groups on standardizing aspects of quantum computing, networking and sensing.[140] These efforts cover hardware interfaces, performance benchmarking and security guidelines across both research and industry sectors.

However, quantum standardization is no longer a purely technical process; it has increasingly become a domain of geopolitical competition.[141] China, in particular, has leveraged state-led initiatives, such as a national standardization development outline plan, to expand its influence in international standards-setting bodies.[142] It has been especially active within the ITU-T, promoting proprietary QKD protocols with the goal of shaping global network specifications in its favour.[143] In response, the USA advocated for the creation of a new, broad ISO/IEC JTC on quantum technologies.[144] Moreover, by positioning the US government—rather than industry—as the lead representative in this new committee, the approach departs from the traditional US model of private sector-led standards development, which has often been praised for its technical neutrality and alignment with industry expertise. This shift raised concerns among stakeholders about the risk of politicizing standards development, echoing criticisms previously directed at state-led approaches.[145]

These tensions highlight a broader strategic risk: analysts caution that, if quantum standardization efforts become increasingly fragmented along geopolitical lines, it could lead to 'standardization wars' that undermine global security, delay technological adoption and entrench incompatible technological ecosystems.[146] Just as past rivalries over telecommunications and semiconductor standards influenced the global technology landscape, poorly coordinated efforts in quantum could have long-term consequences. Therefore, while active participation in international standardization bodies remains important, it should be accompanied by careful coordination among trusted partners. Rather than premature or politicized interventions, emphasis should be placed on promoting robust, transparent and inclusive standards—to support resilient supply chains, safeguard sensitive data and help maintain the technological competitiveness of states in the emerging quantum domain.

[139] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), 'ISO/IEC DIS 23837-1:2023—Information security—Security requirements, test and evaluation methods for quantum key distribution—Part 1: Requirements', Aug. 2023.

[140] IEEE Standards Association, 'IEEE standards & projects for quantum technologies', [n.d.].

[141] Zúñiga, N. et al., 'The geopolitics of technology standards: Historical context for US, EU and Chinese approaches', *International Affairs*, vol. 100, no. 4 (July 2024).

[142] Xinhua, [The Central Committee of the Chinese Communist Party and the State Council issue the national standardization development outline], Chinese State Council, 10 Oct. 2021 (in Chinese).

[143] Center for Intelligence Research and Analysis (CIRA), *A New 'Great Game'?: China's Role in International Standards for Emerging Technologies* (Exovera: Reston, VA, Aug. 2022).

[144] International Electrotechnical Commission (IEC), 'IEC/ISO JTC 3 quantum technologies', [n.d.].

[145] Cory, N., 'The Biden administration overreacts responding to China's role in setting standards for quantum technologies', Innovation Files, Information Technology & Innovation Foundation, 29 July 2024.

[146] Zúñiga et al. (note 141).

7. Conclusions and recommendations

Quantum technologies are moving beyond theoretical exploration and starting to influence the strategic landscape across the military, intelligence and critical infrastructure domains. Their unique capabilities—such as secure communications, precision sensing and advanced computation—are being explored not only for their technical promise, but also for their implications for deterrence, arms control, surveillance and operational resilience. While most applications remain in early or pilot phases, the direction of development is clear: quantum systems are becoming embedded in the future of national and international security planning.

What makes quantum technologies distinct from previous waves of innovation is their potential to reshape technical and informational structures—altering what can be sensed, predicted or protected. Unlike technologies that enhance firepower or mobility, quantum advances may redefine how knowledge is secured and applied across time and space. This creates new opportunities for secure infrastructure and verification, but it also risks destabilizing long-standing security assumptions. The uneven and unpredictable pace of quantum progress—across states, alliances and sectors—adds further urgency to strategic assessments and policy preparedness.

Governments are already responding by embedding quantum into national strategies, funding frameworks, export control regimes and research security initiatives. These responses reflect not only the dual-use character of quantum technologies, but also their geopolitical significance. Investments and collaborations increasingly align with existing security alliances, while standardization and regulation have become contested arenas. At the same time, opportunities remain for cooperative frameworks—particularly in arms control verification, ethical governance and capacity-building for quantum resilience.

As with other emerging technologies, the challenge is to navigate between hype and neglect—to avoid both overreacting to speculative threats and underpreparing for disruptive shifts. The influence of quantum on international security will not arrive in a single moment; it will unfold through cumulative and uneven change. Anticipating these shifts—and shaping them through governance, norms and strategic foresight—will be essential for ensuring that quantum technologies reinforce, rather than undermine, global stability.

As quantum technologies mature, their influence will extend beyond national capabilities to reshape global norms, power structures and technological dependencies. The international community will need to steer this transformation in ways that enhance peace, stability and equitable access. The following trends and recommendations outline key governance priorities for the coming years based on anticipated technological transformations.

High-resolution magnetic and gravity data sets will become strategic assets

Quantum inertial navigation and anomaly-aided positioning systems—especially for submarines, aircraft and autonomous systems—depend on access to accurate magnetic and gravity anomaly maps. These data sets, once considered scientific curiosities, are becoming strategic infrastructure. As these systems move closer to operational readiness, countries with strong geophysical mapping capabilities will enjoy a significant military and intelligence advantage in GNSS-denied environments.

Recommendations

1. States and alliances should treat magnetic and gravity maps as critical national assets and ensure appropriate protection, access management and classification.
2. Regional bodies such as the EU could invest in cooperative mapping initiatives, following models like Copernicus, to jointly generate and maintain strategic geophysical data.
3. The UN or regional forums should explore frameworks for equitable access to geospatial data for peaceful navigation, especially in regions where strategic dependencies could arise.

Quantum decryption capabilities may widen intelligence asymmetries between states with different levels of technological advancement

Upon Q-day, with the emergence of cryptographically relevant quantum computers, many public-key encryption systems currently in use—especially those widely deployed in the Global South—could be compromised. This threat is amplified by harvest-now, decrypt-later strategies already under way. If not addressed, quantum cryptanalysis may lead to long-term intelligence imbalances, erode trust in international communications, and expose less prepared states to strategic coercion or surveillance.

Recommendations

1. Digital cooperation in the UN and regional bodies should initiate global capacity-building programmes to help developing countries adopt post-quantum cryptography for critical systems.
2. Advanced states and international donors should embed PQC support into digital development initiatives, including funding, training and open-source tools.
3. Multilateral dialogues (e.g. the Global Forum on Cyber Expertise or the UN open-ended working group on information and communications technology) should integrate quantum cryptographic threats into their strategic risk frameworks.

The strategic impact of quantum will depend on its integration with other technologies, not on quantum systems alone

The most transformative applications of quantum are likely to arise from its convergence with other emerging and disruptive technologies, such as AI, autonomy and space systems. This quantum + *X* paradigm will shape military innovation in diverse areas including decision making, swarming, stealth, secure satellite links and cognitive sensing. However, integration challenges—technical, organizational and ethical—may limit the real-world impact of isolated quantum breakthroughs.

Recommendations

1. Governments and funding agencies should design quantum programmes to explicitly encourage interdisciplinary collaboration—especially with AI, autonomous systems and space research—to anticipate both risks and opportunities arising through the many quantum + *X* combinations.

2. International research networks could be supported to develop open standards and ethical frameworks for convergence of quantum and emerging and disruptive technologies.
3. Scientific advisory bodies under arms control regimes may wish to monitor how integrated systems affect existing legal norms, verification, and the balance between autonomy and control.

Dual-use quantum development will accelerate and attempts to fully separate civilian and military pathways are unlikely to succeed

Quantum technologies—especially in sensing, communications and simulation—are inherently dual-use. As commercial platforms grow more capable, military and intelligence services are increasingly sourcing components, expertise and platforms from civilian markets. Attempts to fully decouple civilian and military pathways risk hampering innovation and deepening global asymmetries.

Recommendations

1. Governments and regional groups should acknowledge the dual-use character of quantum technologies and develop proportionate governance frameworks—including export controls, research security and ethics.
2. Defence innovation initiatives, such as NATO's Defence Innovation Accelerator for the North Atlantic (DIANA) or the EU's European Defence Fund, should be matched by civilian oversight and transparency tools.
3. Scientific communities and industry consortia should be encouraged to adopt voluntary ethical codes for dual-use quantum development.

National self-sufficiency in quantum technologies is unrealistic—international cooperation is necessary for resilience and innovation

Quantum technology ecosystems rely on highly specialized and geographically dispersed supply chains, including cryogenics, rare isotopes, superconducting circuits, high-purity optics and nanofabrication. No single state controls all of the capabilities needed to build scalable quantum systems. As a result, international cooperation—especially among trusted partners—is not just advantageous, but essential to resilience.

Recommendations

1. States with active quantum programmes should strengthen bilateral and multilateral supply chain cooperation to reduce chokepoints and dependency risks.
2. International organizations such as the UN Institute for Disarmament Research (UNIDIR), the Organisation for Economic Co-operation and Development (OECD) or the World Trade Organization (WTO) could support global supply chain mapping and resilience frameworks.
3. Emerging economies should be supported with access to critical materials, training and technology-sharing agreements to prevent deepening global technological divides.

There is a growing need for dedicated institutions to assess the peace and security implications of quantum technologies

While attention to the ethical and social impacts of quantum science is increasing, few institutions currently focus on the strategic, arms control or geopolitical consequences. The dual-use nature of many quantum technologies—especially in sensing and intelligence—requires new frameworks to evaluate how quantum may affect international and human security, transparency and global stability.

Recommendations

1. International capacities should be established, with interdisciplinary expertise and unattached to a single country or alliance, to effectively monitor risks and opportunities of quantum technologies for international peace and security.
2. Relevant multilateral institutions, such as those focused on arms control, disarmament or strategic stability, should integrate quantum monitoring into their scientific and technical advisory processes.
3. Academic networks could be supported to foster cross-disciplinary training in quantum policy, security and ethics.

Malicious or illicit use of quantum technologies by non-state actors is likely to emerge over time

As quantum systems become smaller, cheaper and increasingly open-source, non-state actors—including criminal organizations and state-aligned proxies—may acquire or develop basic quantum tools. Early threats may include uses of quantum for secure communications, evasion of surveillance or cryptographic attacks. Eventually, more advanced capabilities could be co-opted or repurposed for surveillance, intrusion or sabotage.

Recommendations

1. Law enforcement agencies globally should begin preparing for quantum-related threats through training, coordination and capability development.
2. International police organizations, such as Interpol and Europol, should create specialized working groups to anticipate and track quantum misuse.
3. Donor states and scientific networks could support ethical self-governance in open-source quantum communities and invest in early detection tools for misuse scenarios.

Appendix A. Glossary

Blind quantum computing	Delegation of a computation to a quantum server without revealing the input, algorithm or output
Boson sampling	A specialized quantum task in which identical photons are sent through an optical circuit, and the pattern of where they end up is measured; while hard for classical computers to simulate, it is not useful for general-purpose computing
Circuit layer operations per second (CLOPS)	A metric to measures the performance of a quantum computer *See also* Reliable quantum operations per second; Quantum volume
Cryogenic quantum computing	The cooling of qubits close to absolute zero (–273.15 °C or 0 K) to minimize thermal noise and extend coherence; some qubits (e.g. superconducting or spin qubits) must be cooled in dilution refrigerators, while others (e.g. trapped ion or neutral atom) use laser cooling instead
Cryptographically relevant quantum computer (CRQC)	A quantum computer capable of decrypting a widely used asymmetric encryption method *See also* Q-day
Distributed quantum computing	Connecting multiple quantum processors over quantum links so that they cooperate on a single computation
Entanglement	The non-local correlation of the state of one qubit to the state of another, no matter how far apart they are—a change in the state of one instantly affects the other; measurement of one provides immediate information about the other *See also* Quantum correlation
Fidelity	A measure of how close a quantum state or operation is to its ideal or expected version; a fidelity of 1 means perfect agreement with the target state or operation, while lower values indicate deviations due to noise, errors or imperfections
First quantum revolution	Technologies based on the collective behaviour of large numbers of quantum particles (e.g. in a semiconductor or a laser)
Fixed qubit	A stationary qubit manipulated by sequences of logic gates *See also* Gate-based model
Flying qubit	A particle (e.g. a photon) that moves through a circuit and is measured along the way *See also* Measurement-based model
Gate-based model	A quantum computing system that manipulates stationary, fixed qubits using sequences of logic gates
Grover's algorithm	A quantum algorithm for unstructured search (e.g. in an unsorted data set) with quadratic speed-up over any classical search
Harvest-now, decrypt-later (HNDL)	A strategy whereby encrypted communications (public key and encrypted data) are intercepted and stored today with the aim of decrypting them once CRQCs become available *See also* Q-day
Hybrid computing	Use of quantum hardware only for targeted subtasks, with the classical computer performing the bulk of the computation and all orchestration tasks

Logical qubit	An error-corrected unit of quantum information built from multiple physical qubits to ensure reliability over time *See also* Quantum error correction
Measurement-based model	A quantum computing system that measures flying qubits as they move through a circuit
Networked quantum sensing	Entanglement of spatially separated quantum sensors to improve sensitivity or resolution beyond what is possible individually
Neutral-atom qubit	Encoding quantum states by laser-cooling individual neutral atoms and holding them in optical tweezers or lattices
Nitrogen-vacancy (NV) centre	Engineered defects in diamond crystals that respond to radio-frequency signals under the influence of magnetic fields and vice versa, producing changes in fluorescence that can be read optically
No-cloning theorem	The impossibility of creating an exact copy of an arbitrary unknown quantum state
Noisy intermediate-scale quantum (NISQ) device	A typical contemporary quantum system with tens to hundreds of imperfect qubits and limited fidelity
Phase relationship	The relative difference in phase between quantum states or wave components, which affects how they interfere *See also* Entanglement; Quantum interference; Superposition
Photonic qubit	A qubit encoded in light modes, either as discrete single photons or as continuous-variable states, manipulated with linear optics, squeezers and measurements for measurement-based quantum computing
Physical qubit	A real two-level quantum device (e.g. superconducting, trapped ion or spin) that holds one qubit of information but is prone to errors, requiring many such qubits for error-corrected logical operations
Post-quantum cryptography (PQC)	New classical cryptographic algorithms believed to resist both classical and quantum attacks *See also* Quantum cryptography
Precise time transfer	Use of entangled quantum states to synchronize clocks at distant locations
Q-day	The moment when a quantum computer is powerful enough to break RSA-2048 encryption *See also* Cryptographically relevant quantum computer
Quanta	The smallest possible units of certain physical properties (e.g. the energy levels of an atom, the spin of an electron, the polarization of a photon)
Quantum advantage	When a quantum computer solves a problem with real-world applications (e.g. in chemistry, optimization or machine learning) faster or more efficiently than classical methods *See also* Quantum supremacy
Quantum algorithm	A step-by-step procedure designed to run on quantum computers
Quantum annealer	A quantum device designed to solve optimization problems by encoding them as an energy landscape and exploiting quantum tunnelling to find the lowest-energy solution

Quantum coherence	The ability of a quantum system to maintain a well-defined phase relationship, enabling superposition and interference
Quantum communications	The use of quantum mechanical principles to develop secure and advanced services for quantum information transfer over quantum networks *See also* Quantum networks
Quantum correlation	Statistical connections between quantum systems that go beyond classical probabilities (e.g. entanglement)
Quantum cryptography	Applying the principles of quantum physics to enhance security of communications *See also* Post-quantum cryptography
Quantum diamond microscope (QDM)	A device that uses diamond crystals embedded with nitrogen vacancy centres to detect defects or malicious modifications in microchips by sensing variations in magnetic fields
Quantum error correction (QEC)	Techniques that protect quantum information from noise and errors by encoding a more stable 'logical qubit' across many physical qubits without directly measuring and disturbing the quantum state
Quantum gate	An elementary unitary operation acting on one or more qubits to change their quantum state, serving as the building blocks of quantum circuits *See also* Quantum operation
Quantum ghost imaging	Reconstruction of an image using correlations between entangled photons—one detected after interacting with the object (without spatial resolution), the other used to form the image
Quantum illumination	Use of quantum correlations to distinguish weak signals from noise, enhancing object detection in cluttered environments
Quantum imaging	Use of specially prepared light (often involving entangled or squeezed photons) to illuminate an object and detect the returning signal, enabling imaging with higher resolution, better contrast or greater sensitivity
Quantum inertial navigation	Application of the principles of quantum mechanics (in particular atom interferometry) to create interference patterns that can measure acceleration and rotation with exceptional precision
Quantum interference	When quantum particles exist in multiple states or paths at once, and these possibilities combine to increase or cancel the chance of certain outcomes
Quantum key distribution (QKD)	Use of quantum properties of particles (typically photons) for the secure exchange of an encryption key that can then be used to protect classical data using standard encryption methods
Quantum machine learning	Use of quantum computers to enhance or accelerate machine learning tasks by leveraging quantum properties
Quantum magnetometry	Use of quantum systems to measure magnetic fields with extremely high precision, leveraging quantum such effects as superposition and entanglement for enhanced sensitivity
Quantum measurement	The process of extracting information from a quantum system, which typically disturbs the system and collapses its state from a superposition to a definite outcome

Quantum memory	A device that stores quantum information for later retrieval, enabling synchronization in quantum networks and quantum repeaters
Quantum metrology	Use of coherence and entanglement to improve precision in measuring time, frequency and other units
Quantum network	A system designed to transmit quantum information, typically encoded in single photons, that can travel through optical fibre or free-space links (e.g. using satellites) *See also* Quantum communications
Quantum noise	Unwanted interactions that disrupt qubit states and cause errors in calculations or communications
Quantum operation	Any physical process that changes the state of a quantum system, including quantum gates, measurements or interactions with the environment *See also* Quantum gate
Quantum processing unit (QPU)	The core hardware unit in a quantum computer, analogous to the CPU in a classical system
Quantum random number generator (QRNG)	Use of quantum processes (e.g. detection of individual photons or quantum algorithms in quantum computers) to generate random numbers that are fundamentally unpredictable
Quantum repeater	An intermediate node that helps extend quantum communications over long distances by dividing the channel into segments and using entanglement swapping and quantum memory *See also* Trusted repeater
Quantum secret sharing	A message split among several recipients that can only be revealed when they cooperate
Quantum secure direct communication	Secure transmission of information over a quantum channel without first generating a key
Quantum sensing	Use of quantum systems to measure physical quantities (e.g. magnetic fields, electric fields, temperature or acceleration) with very high sensitivity
Quantum simulators	A specialized device built to replicate and study specific quantum systems found in nature (e.g. molecular interactions)
Quantum state	The fundamental condition of a quantum system (e.g. an electron or a photon), containing all the possible information about the system, including such properties as energy, spin or polarization *See also* Entanglement; Superposition
Quantum supremacy	The point at which a quantum computer can solve a specific problem (not necessarily useful) that is infeasible for any classical computer *See also* Quantum advantage
Quantum technologies	Technologies that involve the ability to control and use individual quantum systems (e.g. single atoms, electrons or photons)
Quantum tunnelling	A quantum phenomenon whereby a particle, due to its wave-like nature and the probabilistic rules of quantum mechanics, can pass through an energy barrier it classically should not be able to cross

Quantum volume	A metric to measures the performance of a quantum computer *See also* Circuit layer operations per second; Reliable quantum operations per second
Qubit	Quantum bit, the basic unit of information in quantum computing that, unlike classical bits (which are either 0 or 1) can leverage quantum effects to perform more complex operations *See also* Fixed qubit; Flying qubit; Logical qubit; Neutral-atom qubit; Photonic qubit; Physical qubit; Silicon qubit; Superconducting qubit; Trapped-ion qubit
Reliable quantum operations per second (rQOPS)	A metric to measures the performance of a quantum computer *See also* Circuit layer operations per second; Quantum volume
Rydberg atom	An atom excited to a highly sensitive energy state that responds to an external radio-frequency field by shifting its internal state and emitting a detectable optical signal
Second quantum revolution	*See* Quantum technologies
Shor's algorithm	A quantum algorithm for factoring integers
Silicon qubit	*See* Spin qubit
Spin qubit	A qubit encoded in the spin of a single electron, typically confined in a quantum dot or similar nanoscale structure, and controlled using magnetic or electric fields
Squeezed photon	A photon with reduced quantum noise, which allows it to be more precisely measured
Superconducting quantum interference device (SQUID)	A highly sensitive device that uses superconducting loops to detect very small magnetic fields, based on quantum interference effects
Superconducting qubit	A qubit built from tiny superconducting circuits where current or voltage represents quantum states, controlled by microwave pulses and operated at cryogenic temperatures for stability
Superposition	The property of a qubit that allows it to be in a combination of states at the same time, not just one, enabling quantum computers to perform many calculations in parallel; when measured, the superposition collapses into just one of the possible outcomes
Trapped-ion qubit	A qubit encoded in the internal energy levels of a single ion held in place by electromagnetic fields, manipulated with lasers for high precision and long coherence times
Trusted repeater	An intermediate node that decrypts and re-encrypts a quantum key before forwarding it *See also* Quantum repeater
Universal quantum computer	Systems that use quantum gates (quantum operations) to solve a wide range of problems using either fixed or flying qubits
Verification	Ensuring that computations are performed correctly and that the outputs are trustworthy

About the author

Dr Michal Krelina is an associate senior researcher with the SIPRI Armament and Disarmament research area. He also co-founded and serves as chief technology officer for QuDef, a quantum security company, and is a research scientist at the Czech Technical University in Prague. His professional interests span mapping military applications of quantum technologies, exploring their roles in future conflicts, developing quantum countermeasures, assessing quantum technology risks and threats, examining the convergence of quantum and classical cybersecurity, and studying the impact of quantum technology on international security and peace research. His recent publications include 'The prospect of quantum technologies in space for defence and security', *Space Policy* (2023), and 'An introduction to military quantum technology for policymakers' (SIPRI, 2025).

STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE
Signalistgatan 9
SE-169 72 Solna, Sweden
Telephone: +46 8 655 97 00
Email: sipri@sipri.org
Internet: www.sipri.org