SIPRI Background Paper
March 2025

AN INTRODUCTION TO MILITARY QUANTUM TECHNOLOGY FOR POLICYMAKERS

MICHAL KRELINA

SUMMARY

● Quantum technology, based on quantum mechanics, is undergoing a 'second quantum revolution' that focuses on controlling individual particles to unlock disruptive applications in computing, communications and sensing. These advances promise major military and security benefits—such as ultra-secure communications, enhanced battlefield sensing and optimized logistics—but they also carry risks if adversaries gain a technological edge.

Governments worldwide are heavily investing in quantum research and development, reflecting its dual civilian and military nature. However, current systems remain error-prone and limited in scalability, while there are concerns over potential misuse. Moreover, key gaps persist in understanding how quantum tools might reshape arms control verification and international security.

Given the rapid pace of development, proactive policymaking and appropriate oversight measures are essential to harness quantum technology's benefits while mitigating its risks.

Quantum technology has quickly become a topic of keen interest for governments, military institutions and private industry. After more than a century of research into quantum mechanics, a 'second quantum revolution' is taking place that focuses on controlling the quantum properties of individual particles—such as electrons and photons. This shift from merely understanding quantum systems to deliberately engineering them has opened up new frontiers in computing, communications, sensing and more that could be applied in ways that disrupt international security. For policymakers, the stakes are high: quantum innovations offer major advantages for defence and security—from secure communications to advanced sensing—but they also pose significant risks if adversaries achieve a technological edge.[1]

This background paper aims to provide a clear, concise overview of military-relevant quantum technology. It begins (in section I) by explaining what quantum technology is and why it differs so much from conventional approaches. It does this by classifying the field into three main categories—quantum computing, quantum communications and quantum sensing—highlighting how each area is advancing and what that might mean for defence. It then (in section II) discusses key military applications that are currently the most advanced or strategically significant—such as secure quantum networks and advanced sensing devices—before turning (in section III) to the broader international security picture. By the conclusions (in section IV), military and security policymakers should understand why quantum technology is strategically important, how it may reshape military capabilities and defence planning, and what steps might be necessary to navigate its rapid development and proliferation.

I. What is quantum technology?

Quantum technology is based on the ideas of quantum mechanics—a theory that was first developed more than a century ago to explain the strange and surprising behaviour of tiny particles such as electrons and photons.[2] In the early 1900s, scientists realized that these particles do not follow the same

[1] Krelina, M. and Jürgen, A., 'Quantum technologies—A new field that needs assessment', *Friedens-Warte*, vol. 95, nos 3–4 (Dec. 2022).

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

* Thanks to the Government of Austria for the generous funding of this paper.

Box 1. Core definitions in quantum technology

Quantum state

A quantum state describes the fundamental condition of a quantum system, such as an electron or a photon. It contains all the possible information about the system, including properties like energy, spin or polarization. Quantum states follow unique principles, such as superposition and entanglement, making them central to quantum computing, communications and sensing.

Quantum bit (qubit)

A quantum bit (qubit) is the basic unit of information in quantum computing. Unlike classical bits, which are either 0 or 1, a qubit can leverage quantum effects to perform more complex operations. Quantum computers use qubits to process information in new ways, enabling faster problem-solving for certain applications, such as cryptography and material simulations.

Quantum superposition

Quantum superposition allows a quantum system—such as a qubit—to exist in multiple quantum states at the same time. This means that a qubit can be a 0 and 1 simultaneously until measured. This principle enables quantum computers to perform many calculations in parallel, providing a potential speed advantage over classical systems.

Quantum entanglement

Quantum entanglement is a phenomenon where two or more quantum particles become strongly correlated, no matter how far apart they are. A change in one particle's state instantly affects the other, even over large distances. This unique property enables ultra-secure quantum communications and is a key factor in quantum computing, networking and sensing.

Noise and quantum error correction

Quantum systems are highly sensitive to their environment, which leads to quantum noise—unwanted interactions that disrupt qubit states and cause errors in calculations or communications. This sensitivity is a major challenge in developing stable and reliable quantum technology. Quantum error correction (QEC) is a set of techniques designed to counteract quantum noise and reduce errors in quantum computations. Unlike classical error correction, QEC requires encoding quantum information across multiple qubits to detect and correct errors without directly measuring and disturbing the quantum state.

rules as everyday objects, leading to groundbreaking discoveries about how nature works at the smallest scales.

From the first half of the 20th century, these findings sparked what is now called the 'first quantum revolution'. By controlling the collective behaviour of many particles, technologies such as nuclear fission, lasers and semiconductors could be developed. These advancements had far-reaching impacts: they led to nuclear weapons and nuclear energy; lasers for barcode scanners, surgery or laser-guided munitions; and modern computers. They also paved the way for important medical applications such as radiology, nuclear medicine and advanced imaging tools that help doctors diagnose and treat diseases.

Although the first quantum revolution continues to evolve and provide new technologies, a second quantum revolution has begun. This involves controlling quantum effects in individual particles—for example, single electrons, atoms or photons—rather than the collective control of groups of them. By working with one particle at a time, scientists can make use of special properties such as superposition (where a particle can be in multiple states at once; see box 1), entanglement (where particles stay connected even when far apart) and the no-cloning theorem (which says that an unknown quantum state cannot be exactly copied).

These new abilities promise major breakthroughs in such fields as computing, communications and sensing. For instance, quantum computers might solve certain problems far beyond the reach of current supercomputers, while quantum communications could allow for ultra-secure data transfer. However, these advancements are not guaranteed—quantum computers remain highly error-prone, and their advantages apply primarily to specific

types of problem (e.g. optimization and material simulations), rather than general-purpose computing. Similarly, while quantum communications offers unparalleled security, scaling up quantum networks to practical, large-scale deployment remains a significant technical challenge. Understanding the possibilities—and their implications for military strategy, intelligence capabilities and military infrastructure—is becoming an increasing priority for policymakers as quantum technology advances.

Key areas of quantum technology

Quantum technology can be grouped into three broad categories: quantum computing, quantum communications, and quantum sensing and imaging. Each category harnesses different quantum effects to overcome key limitations of traditional approaches in computing, communications and sensing—such as processing power, security vulnerabilities and measurement precision. They offer both significant opportunities and new challenges for international security and policymaking.

Quantum computing

Quantum computing uses 'qubits' (quantum bits); these are the fundamental units of quantum information, which can exist in multiple states at once due to superposition. This unique property allows quantum computers to process information in ways not possible with classical, binary systems. Qubits are the foundation of quantum technology, not only in computing but also in quantum communications and quantum sensing, where their special properties enable secure encryption and ultra-precise measurements.

While today's quantum computers are relatively small and prone to errors, experts predict that in the next decade or so there may be systems capable of powerful simulations and calculations.[3] Recent advancements—such as Google's quantum processor Willow, which aims to improve quantum error correction, and Microsoft's Majorana 1, which explores topological qubits for more stable computing—demonstrate steady progress toward more scalable and reliable quantum processors.[4]

Quantum computers could, for example, help design new materials and drugs by simulating chemical reactions and molecular structures more precisely than ever before. These advancements could lead to stronger, more resilient military-grade materials or new medical treatments for battlefield injuries and biothreats. They might also solve complex optimization problems—such as planning efficient supply chains or scheduling military logistics—faster and more effectively than classical systems.

However, this potential power also poses security risks since future quantum computers may be able to break much existing encryption if 'quantum-safe' methods are not adopted. Quantum-safe (or post-quantum) cryptography refers to encryption methods believed to be secure against an attack by a large-scale quantum computer.

[3] QuEra, *Survey Report: Quantum Readiness* (QuEra: Boston, MA, Jan. 2025).

[4] Neven, H., 'Meet Willow, our state-of-the-art quantum chip', Google Quantum AI, 9 Dec. 2024; and Bolgar, C., 'Microsoft's Majorana 1 chip carves new path for quantum computing', Microsoft, 19 Feb. 2025.

Quantum communications

Quantum communications leverages quantum effects to create secure communications channels and potentially build a 'quantum internet'. Currently, the best-known application is quantum key distribution (QKD), in which any attempt at eavesdropping immediately disrupts the transmission, signalling a breach.

But the vision of the quantum internet goes beyond QKD. Researchers are working on advanced quantum communications networks—on earth and via satellites—that could allow new types of secure data transfer, distributed quantum computing and even connected quantum sensors. Such a network may one day support not just unhackable communications but also services such as cloud-based quantum computing, where users access quantum processors over secure quantum links.

Quantum sensing and imaging

Quantum sensing and imaging take advantage of subtle quantum properties to measure physical quantities with extreme accuracy, far beyond what classical instruments can achieve. This includes quantum-enhanced atomic clocks for precise timing; sensitive magnetometers for brain imaging and detection of hardware trojans on chips; gravimeters for detecting submarines, underground structures and minerals; and advanced navigation systems that work without a global navigation satellite system (GNSS) such as the Global Positioning System (GPS).

Another exciting area is quantum imaging, where techniques such as quantum lidar or 'around-the-corner' cameras could detect objects in low light or through obstacles. These innovations could transform military reconnaissance, border monitoring and emergency response, giving a significant advantage to states that develop them early.

Why is there so much hype around quantum technology?

Recently, quantum technology has captured worldwide attention for several reasons, chief among them being its potential to trigger a new wave of scientific and industrial breakthroughs. Governments, corporations and academic institutions all see quantum as a way to push the boundaries of what can be achieved in computing, communications and sensing. Unlike many purely academic fields, quantum research has a direct path to real-world applications—a strong mix of fundamental discoveries, product-oriented development and commercial investments. This combination drives rapid innovation and big promises about how quantum devices might one day transform economies, militaries, security, social relations, healthcare and daily lives.

One major factor behind the hype is the keen interest from both the public and the private sector. Governments are pouring billions of dollars into national quantum initiatives, such as the United States' National Quantum Initiative, China's ambitious quantum research programmes and the Quantum Flagship of the European Union (EU).[5] These programmes are not just funding basic science; they are designed to quickly translate findings

[5] Qureca, 'Quantum initiatives worldwide 2024', 1 Apr. 2024.

into strategic advantages for security, industry and healthcare. In addition to direct funding, governments are coordinating large-scale efforts (e.g. the European Quantum Communication Infrastructure, EuroQCI) to build quantum networks across national borders.[6] Such high-profile commitments signal that quantum technology is seen as a critical arena for international competition and collaboration.

At the same time, commercial giants and start-ups are racing to bring quantum products to market.[7] Large companies such as Alibaba, Amazon, Atos, Google and IBM are investing heavily in quantum computing, while smaller firms are exploring niche applications such as quantum sensors for medical diagnostics or precision manufacturing. Venture capital for promising quantum start-ups is steadily growing, although it remains modest compared to the funding for artificial intelligence (AI).[8] This commercial drive fuels media attention, encourages more academic research and spurs new government policies, thereby creating a self-reinforcing cycle of optimism and high expectations.

Yet, with big promises come big uncertainties. Quantum devices remain difficult to build, and many experts caution that the road to reliable, large-scale systems could take longer than anticipated. Even so, history shows that fundamental breakthroughs can come sooner than expected—and when they do, they often bring significant, sometimes disruptive, surprises.[9] While the exact timeline for transformative quantum applications remains uncertain, research suggests that major scientific advances frequently emerge when focused efforts integrate unexpected elements. For instance, a large-scale study found that breakthrough discoveries often arise from novel combinations of problems, methods and contexts, rather than from purely incremental progress.[10]

Consequently, the hype around quantum technology reflects not only its immense promise, but also the fact that a few unexpected leaps could dramatically reshape security, economies and ways of life. Given this pattern, governments and businesses can ensure that they are not caught off guard by making early preparations—such as investing in quantum-safe encryption, monitoring technological advancements and developing regulatory frameworks. Such preparation will be effective whether breakthroughs arrive in the near future or take longer to materialize.

II. Quantum technology for military applications

Governments and military organizations—armed forces, defence ministries and intelligence agencies—worldwide are investing heavily in quantum research because of the potentially game-changing advantages it could offer in such areas as secure communications, advanced sensing and next-generation computing. While there are many possible military applications, a

[6] European Commission, 'The European Quantum Communication Infrastructure (EuroQCI) initiative', 22 Oct. 2024.

[7] McKinsey & Co., 'Quantum technology monitor', Apr. 2024.

[8] McKinsey & Co. (note 7).

[9] Allnutt, V. et al., 'Great accidental discoveries', Goethe Institut, Aug. 2020.

[10] Shi, F. and Evans, J., 'Surprising combinations of research contents and contexts are related to impact and emerge with scientific outsiders from distant disciplines', *Nature Communications*, 24 Mar. 2023.

few stand out as especially promising—and potentially disruptive—for future military and security strategies.[11]

Prospective military applications

Quantum communications

Quantum communications is often the first area that comes to mind. Beyond the well-known QKD application, quantum networks are expected to enable highly secure data-sharing, precise clock synchronization and even the distribution of highly accurate timing. All these capabilities are valuable for national security, financial systems and critical infrastructure. In a military context, these technologies could enhance secure battlefield communications, improve coordination in contested environments and safeguard command-and-control networks from cyberthreats.

Several states, including China and members of the EU, are experimenting with satellite-based quantum links to extend secure communications across large distances. They view it as both a strategic asset for national security and a potential military advantage in secure operations.[12]

Examples of progress in quantum communications include a 2024 experiment that successfully demonstrated QKD using a system based on uncrewed aerial vehicles (UAVs).[13] This shows the potential for secure wireless communications in mobile military settings, which could lead to highly secure battlefield networks that are resistant to cyberthreats.

Quantum sensing and imaging

Quantum sensing and imaging hold equally transformative potential. Advancements in this area could significantly enhance how militaries gather intelligence, navigate in hostile environments and detect threats.

For example, signals from a GNSS (e.g. the USA's GPS, the EU's Galileo, Russia's GLONASS or China's BeiDou) can be jammed or spoofed by an adversary. Instead, non-GNSS navigation systems based on quantum inertial sensors or magnetic anomaly mapping could allow submarines and aircraft to travel covertly or in contested areas. This is a breakthrough area: in June 2024 the AQNav system, which combines quantum sensing with AI to provide real-time navigation without relying on a GNSS, was announced by SandboxAQ (a US company spun off from Google's owner, Alphabet).[14]

Quantum lidar, 'around-the-corner' and other imaging methods offer innovative approaches for intelligence, surveillance and reconnaissance (ISR), enabling the detection and tracking of hidden or obscured targets. Likewise, quantum radio frequency receivers might improve radar and electronic warfare capabilities, enabling forces to detect faint signals and more effectively jam or evade enemy transmissions.

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

[12] European Commission (note 6); and Kania, E. and Costello, J., 'Quantum leap (part 2): The strategic implications of quantum technologies', *China Brief*, vol. 16, no. 19 (21 Dec. 2016).

[13] Tian, X et al., 'Experimental demonstration of drone-based quantum key distribution', *Physical Review Letters*, 15 Nov. 2024.

[14] SandboxAQ, 'SandboxAQ announces AQNav—World's first commercial real-time navigation system powered by AI and quantum to address GPS jamming', 25 June 2024.

Cybersecurity applications of quantum sensing are also being explored. Germany's Agency for Innovation in Cybersecurity (Agentur für Innovation in der Cybersicherheit, Cyberagentur) has launched a programme investigating how quantum sensors could open new side-channel attacks on microchips.[15]

Quantum computing

Quantum computing has also drawn significant attention from military planners. Although large-scale quantum computers remain under development, smaller or noisy systems already show promise for specialized tasks, such as optimizing complex logistics or mission planning. In the future, more powerful devices could tackle even more challenging simulations, aiding in the design of advanced materials or quantum-enhanced autonomous AI.

Conversely, quantum computers capable of breaking current encryption standards could pose a major security risk if militaries and governments fail to deploy quantum-safe solutions. Similarly, there is a risk from adversaries using quantum computers to develop advanced simulations in order to design stealth or counter-stealth technologies or to develop biological weapons.

As a result, and although today's quantum computers are still limited, military organizations around the world are keeping a close track of progress in quantum computing. As they do so, they are considering both its use for defensive measures and its offensive potential in order to maintain their strategic edge. Examples of the former include upgraded encryption and improved radar-based detection of UAVs.[16] The ways in which future quantum capabilities might support offensive military operations include faster decision-making and more efficient resource management, with researchers investigating how quantum computers could help with satellite tasking and enhance radar cross-section calculations.[17]

National approaches to military quantum technology

Different countries have taken different approaches.[18] Around the globe, quantum programmes often stress the dual-use nature of the technology, recognizing that breakthroughs can benefit both civilian industries and the armed forces.

The United States, for instance, supports quantum research and development (R&D) through such agencies as the Department of Defense and its Defense Advanced Research Projects Agency (DARPA), often in collaboration with leading technology companies (e.g., IBM and Microsoft).[19] China is known for its ambitious national programmes covering quantum

[15] Cyberagentur, 'Side-channel attacks with quantum sensing (SCA-QS)', [n.d.].

[16] Malarvanan, A. S., 'Hybrid quantum neural network advantage for radar-based drone detection and classification in low signal-to-noise ratio', arXiv 2403.02080, 4 Mar. 2024.

[17] Tucker, P., 'The Navy is trying to use quantum computers to task spy satellites', Defense One, 26 Feb. 2024; and Pellerin, T., van Gaalen, R. and Harmanny, R. I. A., 'Radar cross section estimation using the variational quantum linear solver algorithm', *2024 21st European Radar Conference (EuRAD)* (IEEE: Paris, 25–27 Sep. 2024).

[18] Krelina and Altmann (note 1).

[19] US Defense Advanced Research Projects Agency, 'DARPA selects two discrete utility-scale quantum computing approaches for evaluation', 6 Feb. 2025.

communications satellites and large-scale research hubs.[20] The European Union has its Quantum Flagship initiative, which, while primarily civilian, does include projects that could eventually be used by the military. In addition, the EU has a dedicated military-focused quantum effort as part of the European Defence Fund (EDF).[21] The United Kingdom is also a major player, with strong national quantum initiatives that include military-oriented research.[22] Canada is integrating quantum advancements into the modernization of the North American Aerospace Defense Command (NORAD) to improve surveillance and security.[23] Australia, under its Army Quantum Technology Roadmap, is developing quantum applications for military use, particularly in secure communications and sensing.[24] India is exploring military-related quantum technology, with its armed forces playing a role in strategic planning on quantum.[25]

The current industrial technology and geopolitical landscape presents a unique opportunity for quantum technology's dual-use development. Many quantum start-ups generate minimal revenue, making them reliant on government grants and military funding to sustain innovation. In uncertain geopolitical times, this has led to increased support for military applications, accelerating quantum adoption by the military. Quantum research is being actively funded by such programmes as the Defence Innovation Accelerator for the North Atlantic (DIANA) and the Innovation Hub of the North Atlantic Treaty Organization (NATO); the EU's EDF; US agencies such as DARPA and the US Army, Navy and Air Force research laboratories; Defence Research and Development Canada; and India's Defence Research and Development Organisation (DRDO). Similarly, China's armed forces, the People's Liberation Army (PLA), is driving military-focused quantum initiatives, further intensifying global competition.[26]

Expectations are high. Some experts think quantum devices might start yielding practical military advantages within the next few years—especially in sensing or secure communications, where smaller-scale or near-term prototypes can offer meaningful improvements. Others caution that full-scale quantum computing, capable of reshaping cryptography or real-time battlefield decision-making, may be further off. Still, the potential rewards push militaries to stay engaged, invest in talent and watch the evolving quantum landscape closely. The result is a fast-moving, internationally competitive arena where no single country or organization wants to fall behind.

[20] Graps, A., 'China: The quantum technology landscape—Part 3', Quantum Computing Report, 4 July 2022.

[21] European Commission, 'EDF calls for proposals 2024', 2024.

[22] Allison, G., 'Massive British breakthrough in quantum defence tech', UK Defence Journal, 3 Jan. 2025.

[23] Canadian Armed Forces, 'Research and development for NORAD modernization', 22 Nov. 2024.

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

[25] Tyagi, Y., 'Indian defence establishment pushes boundaries with quantum tech and AI integration at NTN-2024', Republic, 8 Nov. 2024.

[26] Parker, E., 'The Chinese industrial base and military deployment of quantum technology', Testimony before the US–China Economic and Security Review Commission, Rand Corp., 1 Feb. 2024.

III. The role of quantum technology in international security

Geopolitics as a driver of quantum technology

Quantum technology has quickly emerged as a key factor shaping international security. States around the world view quantum innovation as a pathway to strategic advantage, especially in defence and intelligence.[27] The abilities to break or reinforce cryptographic systems, detect stealth assets and improve situational awareness hold obvious appeal. As a result, governments are racing to develop cutting-edge quantum capabilities, creating a new domain of geopolitical competition and cooperation.

Rivalries, balanced and imbalanced

A major dynamic in this domain is the competition between China and the United States.[28] Both countries devote substantial resources to quantum research and have achieved notable milestones, from China's quantum communications satellites to the USA's advanced quantum processors. While it is challenging to pinpoint which country leads in every quantum subfield—given the secrecy surrounding military-related R&D—it is clear that both states aim to prevent the other from being the first to achieve a game-changing breakthrough.

To prevent an opponent from gaining a decisive lead in quantum technology, some states implement various measures such as export controls, investment restrictions and visa policies to limit the transfer of sensitive technologies. For instance, the US Department of Commerce has imposed export controls on quantum computing technology, including key equipment, materials and software used in quantum computers, as well as certain high-performance computing microchips.[29] In additional, the US Department of the Treasury has issued regulations prohibiting specific US investments in China's quantum technology sector in order to prevent China from making advancements that could enhance its military and intelligence capabilities.[30] Similarly, China has tightened domestic control over its quantum research and has implemented measures to restrict foreign collaborations in certain high-security areas.[31]

Overall, the China–USA rivalry drives large-scale national programmes and fosters domestic collaboration among government agencies, private companies and academic institutions.[32] In turn, it sets the pace for other countries seeking to keep up.

In contrast to the relatively balanced China–USA contest, there are regions where quantum asymmetries are more pronounced. A prime example is the

[27] Krelina and Altmann (note 1); and Jacobs Gamberini, S. and Rubin, L., 'Quantum sensing's potential impacts on strategic deterrence and modern warfare', *Orbis*, vol. 65, no. 2 (spring 2021).

[28] Parker E. et al., *An Assessment of the US and Chinese Industrial Bases in Quantum Technology* (Rand Corp.: Santa Monica, CA, 2022); and Parker (note 26).

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

[30] Swayne, M., 'US restricts quantum tech investments in China, citing national security risks', Quantum Insider, 29 Oct. 2024.

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

[32] Hudson, R. L. and Zubașcu, F., 'Science goes to war: Western allies step up collaboration in military research', Science Business, 7 Apr. 2022.

relationship between India and Pakistan.[33] India, with its stronger research infrastructure and economic resources, is investing significantly in quantum projects, from quantum computing initiatives to QKD pilots. Pakistan, in contrast, has more limited resources and is making slower progress in the quantum realm. This may heighten security concerns in the region if India's advantages translate into superior surveillance, secure communications or advanced weapon research. A key open question is whether such a disparity in quantum technology capabilities could influence the nuclear posture of these two nuclear-armed states. For example, advances in quantum sensing could enable more precise submarine tracking, potentially undermining the survivability of nuclear deterrents and destabilizing strategic stability.[34] The impact of quantum technology on nuclear stability remains a significant and largely unexplored question, with research still in its early stages.[35]

Cooperation, bilateral and multinational

Beyond national programmes, bilateral partnerships are playing a significant role in advancing quantum technology. For example, the USA has made joint statements on collaboration with allies such as Australia, Denmark, Germany, Japan, South Korea, the United Kingdom and others.[36] Similarly, partnerships such as that between Australia and India focus on shared quantum R&D initiatives to strengthen technological cooperation in order to address regional security challenges.[37]

Quantum technology has also begun to influence broader alliances and cooperative frameworks. Multinational projects such as the EU's Quantum Flagship and the EuroQCI initiative underscore that some countries see benefit in pooling resources and expertise. Similar collaborations are emerging within the trilateral alliance between Australia, the UK and the USA (AUKUS), where quantum activities are a key focus.[38] AUKUS members are working together to develop advanced quantum technology for their militaries, including quantum sensing, secure communications and potentially quantum computing.

While China, India and Russia have long prioritized national quantum programmes, recent initiatives among members of the BRICS partnership (a 10-state intergovernmental organization that they initiated alongside Brazil and South Africa) suggest increasing cooperation. For example, China and Russia have jointly tested a hack-proof quantum communications link, demonstrating a potential framework for secure data exchange between strategic partners.[39] Similarly, China has established a quantum satellite

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

[34] E.g. Erästö, T., Su, F. and Wan, W., *Navigating Security Dilemmas in Indo-Pacific Waters* (SIPRI: Stockholm, June 2024), pp. 16–17.

[35] Sokova, E., 'Disruptive technologies and nuclear weapons', *New Perspectives*, vol. 28, no. 3 (Sep. 2020); and Fetter, S. and Sankaran, J., 'Emerging technologies and challenges to nuclear stability', *Journal of Strategic Studies*, published online 11 Dec. 2024.

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

[37] Gill, P., 'India and Australia pump $12.7 million into AI, quantum computing and robotics—Renewing their cyber and critical technology partnership', Business Insider India, 4 June 2020.

[38] Munro, B. and Paci, T., 'AUKUS must focus on quantum policy, not just the technology', The Strategist, Australian Strategic Policy Institute (ASPI), 1 Mar. 2023.

[39] Bela, V., 'China and Russia test "hack-proof" quantum communication link for BRICS countries', *South China Morning Post*, 30 Dec. 2023.

link with South Africa, with claims that it intends to leverage its quantum satellites to enable secure communications across the BRICS bloc.[40] These emerging collaborations further illustrate the global momentum in quantum research and signal that emerging economies are beginning to pool resources and expertise.[41] This has the potential to enhance regional security and drive economic collaboration through advanced quantum technology.

Arms control, legal challenges and research gaps

Despite growing investments in research on military quantum applications, key gaps remain. Among others, there are gaps in understanding how quantum technology could aid verification and arms control and how it might be misused in military contexts. While discussions often focus on breaking existing encryption using quantum computer or criminals exploiting QKD, there is little research on how quantum sensing, computing or communications could bypass existing security measures or disrupt military operations. For example, if a non-state actor or a rogue state were to gain access to high-precision quantum sensors, it could use them to improve clandestine surveillance, detect hidden military assets or enhance electronic warfare tactics such as radar jamming and stealth evasion. Likewise, quantum-assisted materials science could accelerate the development of new stealth coatings, armour or explosives before detection mechanisms can adapt.

At the same time, quantum technology could enhance arms control verification, yet its role remains poorly explored. For instance, quantum sensors might one day detect subtle signals of nuclear tests or monitor concealed weapons with greater sensitivity than current methods. However, significant questions remain regarding their practical feasibility, deployment challenges and the overall advantage they might offer. This gap underscores the need for focused research to determine how quantum-enhanced verification could be effectively applied in nuclear arms control.

Current arms control frameworks do not account for the above risks and opportunities. The strategic importance of quantum technology raises questions for arms control, export controls and international law.[42] This makes deeper exploration essential to ensure that quantum advancements do not outpace regulatory oversight. Existing agreements may not adequately address quantum-specific threats, such as a future quantum computer's ability to break widely used encryption.

This is exemplified by the multilateral Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. Its export control lists—which have been adopted and applied by most states with advanced quantum industries—already capture some quantum technology with military applications or security implications, such as quantum

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

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

[42] Abdikhakimov, I., 'Quantum computing regulation: A global perspective on balancing innovation and security', *Journal of Intellectual Property and Human Rights*, vol. 3, no. 8 (Aug. 2024); and Perrier, E., *Quantum Information Technologies and Public International Law: A Strategic Perspective*, Stanford Center for RQT Research Series no. 3 (Stanford Law School: Stanford, CA, Dec. 2024).

cryptography and quantum sensors.[43] However, Russia (one of the Wassenaar Arrangement's 42 participating states) has blocked attempts to adopt new controls that can capture quantum technology.[44] Several states have adopted such new controls at the national level, but their coverage and the patchwork nature of their adoption have sparked concerns among companies and academics working in this space.[45]

Moreover, the integration of quantum technology into military systems introduces ethical considerations. These include the risk of enhanced surveillance capabilities infringing on privacy rights and the possibility of creating new forms of chemical or biological weapons through advanced molecular simulations. This has led to calls for new ethical governance frameworks.[46]

IV. The need for proactive policymaking

Quantum technology is rapidly evolving into a strategic enabler for defence and security, with implications beyond encryption. Quantum sensing, communications and computing offer both opportunities and risks, influencing everything from secure military networks to intelligence and surveillance. While some capabilities, such as quantum communications and quantum-enhanced navigation, are emerging, the long-term impact of quantum computing and advanced sensing on warfare and global stability remains uncertain.

As quantum technology advances, international bodies may consider new treaties or may update existing ones to address the unique challenges that it poses. This could involve agreements that prevent the development of quantum code-breaking capabilities or frameworks that mandate transparency in quantum research. It might involve closer cooperation with the scientific community, perhaps through the creation of a scientific advisory body like that of the Organisation for the Prohibition of Chemical Weapons (OPCW). Given the risks described above, international arms control frameworks such as the 1993 Chemical Weapons Convention (CWC) and the 1972 Biological Weapons Convention (BWC) should begin considering how quantum advancements could have an impact on their scope and effectiveness. While discussions on the potential threats posed by quantum technology and their arms control implications are still in preliminary phases, the rapid pace of quantum R&D indicates that policymakers need to be proactive in shaping new regulatory frameworks before the technology matures further.[47]

Ultimately, the role of quantum technology in international security is evolving alongside the technology itself. The dual-use nature of quantum technology—with applications in both civilian and military domains—

[43] European Commission, 'Emerging technologies developments in the context of dual-use export controls', Fact sheets, Nov. 2020.

[44] European Commission, 'White Paper on export controls', COM(2024) 25 final, 24 Jan. 2024.

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

[46] 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.

[47] SIPRI and Quantum Delta NL, 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.

amplifies its strategic importance. The outcomes of quantum technology's evolving integration into national security will depend on how quickly meaningful quantum devices become practical, as well as how states choose to collaborate—or compete—in leveraging them. For now, the broad consensus is that quantum capabilities and their rapidly advancing military and security applications are too critical to ignore. They promise to reshape everything from communications security to intelligence gathering, influencing both the balance of power among states and also, and perhaps more importantly, national security. This will compel governments to carefully navigate the next phase of technological competition.

Policymakers must act now to harness the benefits of quantum technology while mitigating its risks—before the security landscape is irreversibly reshaped.

Abbreviations

AI	Artificial intelligence
AUKUS	The trilateral alliance between Australia, the United Kingdom and the United States
DARPA	Defense Advanced Research Projects Agency (United States)
EDF	European Defence Fund
EU	European Union
EuroQCI	European Quantum Communication Infrastructure
GNSS	Global navigation satellite system
GPS	Global Positioning System
ISR	Intelligence, surveillance and reconnaissance
QKD	Quantum key distribution
R&D	Research and development
UAV	Uncrewed aerial vehicle

RECENT SIPRI PUBLICATIONS

Parameters to Assess Escalation Risks in Space
Nivedita Raju
2025 February

Bias in Military Artificial Intelligence
Dr Alexander Blanchard and Laura Bruun
2024 December

Enhancing Cyber Risk Reduction and the Role of the European Union
Larisa Saveleva Dovgal, Fei Su and Dr Lora Saalman
2024 December

The SIPRI Top 100 Arms-producing and Military Services Companies, 2023
Lorenzo Scarazzato, Dr Nan Tian, Dr Diego Lopes da Silva, Xiao Liang and Katarina Djokic
2024 December

Critical Minerals and Great Power Competition: An Overview
Dr Jiayi Zhou and Dr André Månberger
2024 October

Mapping the Spread of NewSpace Companies Developing, Testing, Producing or Marketing Missile-related Technology: A Pilot Study
Kolja Brockmann and Lauriane Héau
2024 October

The Expansion of the NewSpace Industry and Missile Technology Proliferation Risks
Kolja Brockmann and Lauriane Héau
2024 October

Nuclear Weapons and Artificial Intelligence: Technological Promises and Practical Realities
Vladislav Chernavskikh
2024 September

Towards a Two-tiered Approach to Regulation of Autonomous Weapon Systems: Identifying Pathways and Possible Elements
Laura Bruun
2024 August

Cyber Risk Reduction in China, Russia, the United States and the European Union
Dr Lora Saalman, Fei Su and Larisa Saveleva Dovgal
2024 June

Reducing the Role of Nuclear Weapons in Military Alliances
Dr Tytti Erästö
2024 June

SIPRI BACKGROUND PAPER

AN INTRODUCTION TO MILITARY QUANTUM TECHNOLOGY FOR POLICYMAKERS

MICHAL KRELINA

CONTENTS

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, Prague. His professional interests focus on the security and defence applications of quantum technology. His recent publications include 'The prospect of quantum technologies in space for defence and security', *Space Policy* (2023), and 'Quantum technologies—A new field that needs assessment', *Friedens-Warte* (2022, co-author).

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

DOI: https://doi.org/10.55163/DRDQ1599