Jul. 2025

Quantum Technologies: Key Advances and Implications for Security in Germany and Europe

Policy Brief by Aaranya Alexander, Florian Klumpp, Jakob Hensing

GPPi
GLOBAL PUBLIC POLICY INSTITUTE

Table of Contents

Overview

Emerging quantum technologies have the potential to transform warfare and information security, as well as raising issues around technology access and exposure to foreign coercion. The field of quantum technology comprises three distinct subfields, each at different stages of development: (1) quantum sensing, (2) quantum communications and (3) quantum computing.[1] Sensing and communications technologies are comparatively close to substantial real-world use, with initial implementations of highly precise sensors and secure communication networks already in place. Quantum computing technology is further away from adoption but carries future risks, especially in terms of creating major cyber vulnerabilities that warrant preventive action.

While the global technology ecosystem varies across these three subfields, the United States and China have achieved the greatest progress across the board and have proven most capable of driving technological development to serve their national interests. The security-minded approach adopted by these two actors has amplified the imperative for other nations to develop their own active quantum strategy. Overall, the field is strongly shaped by public funding, a significant share of which is explicitly directed toward advancing military applications, enhancing cybersecurity and strengthening domestic independence and control in the quantum stack.

The European Union and some of its member states (including Germany) play an important role in academic research and in the manufacturing of certain critical components. However, despite their scientific strength, they have struggled to assert themselves as a competitive power when leveraging quantum technologies for practical use, be it commercially or for defense and security sector applications. The new EU Quantum Strategy published in July 2025 aims to address this challenge, seeking to make Europe a global quantum leader by 2030.

German and EU policymakers have taken initial steps to navigate the security challenges and seize opportunities that will arise from quantum technologies in the coming years. These steps are a good start, but more remains to be done. This paper explores and clarifies the evolving risk landscape from a German and European perspective, drawing on public research, policy and market analyses and official government strategies. It serves to underscore in which areas Germany and Europe should further intensify their efforts to ultimately play a more prominent role in the field of quantum technologies.

Understanding Quantum Technologies

When observed at the nanoscale, particles are governed by quantum physics and acquire unique properties that are leveraged in quantum technologies. At their core, quantum technologies make use of the following principles:[2]

[1] Krelina, M., 2021, "Quantum Technology for Military Applications," *EPJ Quantum Technology* 8, no. 24, https://doi.org/10.1140/epjqt/s40507-021-00113-y.
[2] OECD, 2025, "A Quantum Technologies Policy Primer," https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/01/a-quantum-technologies-policy-primer_bdac5544/fd1153c3-en.pdf.

- **Entanglement:** Particles can be intrinsically connected in a manner that spans long distances, allowing for instantaneous data sharing and detection of remote changes.

- **Superposition**: Particles can take on multiple physical states simultaneously (as some might recognize from the well-known "Schrödinger's cat" analogy). This phenomenon means quantum systems can hold exponential amounts of data points simultaneously, potentially allowing bulk information storage and advanced, efficient calculations. Manipulating quantum data is difficult, which makes it useful for security applications but also poses practical challenges.

- **Tunneling**: Particles can move quickly and controllably between specially fabricated nanomaterials, making for faster and more reactive devices.

Quantum Sensing

Quantum sensors either excel at detecting otherwise "invisible" characteristics from a target (e.g., quantum radiation) or use quantum principles to refine a sensor to be sensitive down to the smallest perturbations (e.g., gravitational fields).[3] The wide sensing range and coherence of signals across different environments (water, underground, through interfering magnetic fields) make quantum sensors appealing for defense and environmental applications. For example, a single Rydberg sensor can have a reach of multiple kilometers and can span frequencies that would require hundreds of traditional antennas.[4] Similarly, chemistry and biotechnology benefit from quantum-level optimizations in drug discovery, imaging and personalized medicine.[5] According to the US Quantum Economic Development Consortium (QED-C), in the next five years, quantum biosensors may identify sub-organ abnormalities, test drug efficacy and monitor a body's microbiome or brain waves in real-time.[6] Quantum sensing is the most advanced of quantum developments[7] and is expected to constitute a $1 billion industry by 2028.[8]

Sensing range and signal coherence make quantum sensors appealing for defense and environmental applications.

Quantum Communications

Quantum communication leverages the phenomenon of entanglement to instantaneously send signals over long distances. The largest of such networks have been realized in defense projects using photonic (light) or free space systems,[9] sending signals using a combination of fiber optic cables, satellites and drones. Alternatively, these networks may connect quantum sensors or computers to work collectively to measure and share a broad scope of data.[10] There is also a quantum-specific encryption protocol available (quantum key distribution, QKD) that can send information securely across the interconnects of a quantum network (i.e., between

[3] OECD, 2025, "A Quantum Technologies Policy Primer."
[4] Smith-Goodson, Paul, "Quantum Sensing Unleashed: How Rydberg Sensors Will Disrupt Telecom," *Forbes*, February 20, 2024, https://www.forbes.com/sites/moorinsights/2024/02/20/quantum-sensing-unleashed-how-rydberg-sensors-will-disrupt-telecom/.
[5] OECD, 2025, "A Quantum Technologies Policy Primer."
[6] Quantum Economic Development Consortium (QED-C), 2024, "Quantum Sensing for Biomedical Applications," https://quantumconsortium.org/quantum-sensing-for-biomedical-applications/.
[7] OECD, 2025, "A Quantum Technologies Policy Primer."
[8] Quantum Economic Development Consortium (QED-C), 2025, "State of the Global Quantum Industry 2025," https://quantumconsortium.org/stateofthequantumindustry2025/.
[9] Krelina, 2021, "Quantum Technology for Military Applications."
[10] OECD, 2025, "A Quantum Technologies Policy Primer."

sensors or cables). This protocol is resilient to quantum and classical adversarial attacks,[11] making enhanced cybersecurity an important value-add of quantum communications.

Interconnects for sensors and regional networks (with a span of less than 1,000 km) are closest to deployment in sectors highly reliant on encryption (e.g., finance, defense and data centers), with breakthroughs in transmission range and cost reduction expected to happen before 2030.[12] Increasing cyberthreats and data breaches, as well as the ability to leverage existing fiber optic infrastructure, have already driven the commercialization of limited-range QKD networks by telecommunications companies (including Toshiba and British Telecom's London network[13]). A factor blocking the general adoption of large-scale networks, however, remains the relative ease with which the classical computing options can be scaled and implemented – making the quantum option less attractive in comparison.[14]

Quantum Computing

Quantum computers are isolated systems that can compress, store and manipulate data; these systems are distinct from measuring or sharing devices for sensing and communications. Each computer stores data with qubits (quantum bits) in a manner unique to its architecture. For example, trapped ion computers use the energy state of a rare-earth ion as a qubit, while superconducting qubits use the state of an electron pair travelling in a circuit.

With future discoveries, quantum computers may solve classically unsolvable problems.

Current forefront quantum computers use qubit numbers in the range of 56 (developed by the global forerunner of quantum companies, Quantinuum) with trapped ions to 4,000 (IBM, with superconducting circuits).[15] Those are classified as "noisy-intermediate scale quantum computing devices" (NISQ),[16] alluding to limitations in their calculations' reliability and process capabilities. With future discoveries, quantum computers may solve classically unsolvable problems in a stage known as "fault-tolerant quantum computing" (FTQC).[17] FTQC computers would compute using millions or billions of qubits, with only predictable and correctable errors. Such computers could revolutionize cryptographic and computer science algorithms, with use cases ranging from accelerating medical discoveries to expanding the computing power of AI.[18] However, reaching the FTQC stage still requires overcoming considerable practical obstacles: quantum information is fragile, cannot be copied and requires an extremely controlled environment to keep data intact.[19]

Another open question is how to best gauge and compare the potential of developing systems.[20] Qubit numbers only provide a very partial indication of progress, as some architectures can implement the same algorithm using different numbers of qubits, or scale

---

[11] Krelina, 2021, "Quantum Technology for Military Applications."
[12] Soller, Henning, Yee, Lareina, Bogobowicz, Michael, Zemmel, Rodney, and Gschwendtner, Martina, 2025, "Quantum Communication: Trends and Outlook," McKinsey, https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/quantum-communication-growth-drivers-cybersecurity-and-quantum-computing#/.
[13] British Telecommunications, 2021, "BT and Toshiba to Build World's First Commercial Quantum-Secured Metro Network across London," accessed May 20, 2025, https://newsroom.bt.com/bt-and-toshiba-to-build-worlds-first-commercial-quantum-secured-metro-network-across-london/.
[14] Soller et al., 2025, "Quantum Communication: Trends and Outlook."
[15] Küsters, Anselm, 2025, "Von Superposition zu Superstrategie? Wie die EU ihre neue Politik für Quantentechnologien ausrichten sollte," Centres for European Policy Network, https://www.cep.eu/de/eu-themen/details/von-superposition-zu-superstrategie-wie-die-eu-ihre-neue-politik-fuer-quantentechnologien-ausrichten-sollte.html.
[16] OECD, 2025, "A Quantum Technologies Policy Primer."
[17] Krelina, 2021, "Quantum Technology for Military Applications."
[18] QuEra, 2023, "Understanding Fault-Tolerant Quantum Computing," accessed May 21, 2025, https://www.quera.com/blog-posts/understanding-fault-tolerant-quantum-computing.
[19] Krelina, 2021, "Quantum Technology for Military Applications."
[20] Soller, Henning, Hijazi, Hussein, Gschwendtner, Martina, and Taibah, Reem, 2024, "Enabling the next Frontier of Quantum Computing," McKinsey, accessed May 20, https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/tech-forward/enabling-the-next-frontier-of-quantum-computing.

well with multiple, integrated computers (as opposed to one large one). Metrics can also be incomparable across NISQ architectures, where some systems are more easily manufactured or have more versatile control features.[21]

Importantly, despite quantum computing's eventual promise of vastly enhanced computing capacity, developments in this field are only to a limited extent symbiotic with advances in large language models and frontier AI. Current work on quantum AI focuses mainly on hybrid systems, where a quantum computer can step in to manage bulk data or intensive computations when running a non-quantum AI model.[22] However, the conversion between classical and quantum data requires large amounts of resources. Available systems are poorly scalable, making hybrid quantum AI unlikely before FTQC development.[23] Similarly, current advances in AI have so far not been found helpful in addressing barriers to quantum implementation.[24]

Europe in the Global Quantum Landscape

China and the US are widely seen as the dominant players in quantum technologies. A differentiated assessment of the technology ecosystem, however, shows that Europe also has clear strengths in research and development. Its trailing position is largely due to weaknesses in translating research advances into practical applications. European implementation lacks both the dynamism of private enterprise (backed up by substantial public investment and support) prevalent in the US and the coherence of state-directed action displayed by China. This issue will need to be addressed in future EU strategic quantum policy to realize the continent's potential and tackle a range of security questions as they arise, hand-in-hand with technological advancement.

China and the US are widely seen as the dominant players in quantum technologies.

Global Research and Development Landscape

A 2024 quantum ecosystem analysis by McKinsey found that Europe leads in outputs of fundamental quantum publications (24 percent worldwide) and has a longstanding reputation for a high density of academic quantum talent.[25] Germany plays a prominent role in the field, accounting for 10 percent of publications across the three subfields, notably from the Max Planck Institute for Quantum Optics.[26] TU Delft in the Netherlands is ranked on par with

[21] Küsters, 2025, "Von Superposition zu Superstrategie?"
[22] Widdows, D., Kitto, K., and Cohen T., 2021, "Quantum Mathematics in Artificial Intelligence," *Journal of Artificial Intelligence Research* 72, pp. 1307—41, https://doi.org/10.1613/jair.1.12702
[23] Robles, Nicolas M., Alhajjar, Elie, and Geneson, Jesse, 2024, "Using Artificial Intelligence and Quantum Computing to Enhance U.S. Department of Homeland Security Mission Capabilities," RAND Corporation, https://www.rand.org/pubs/perspectives/PEA2890-1.html; OECD, 2025, "A Quantum Technologies Policy Primer."
[24] Quantum Economic Development Consortium (QED-C), 2025, "State of the Global Quantum Industry 2025."
[25] Bogobowicz, Michael, Dutta, Kamalika, Gschwendtner, Martina, Heid, Anna, Issler, Mena, Mohr, Niko, Soller, Henning, Zemmel, Rodney, and Zhang, Alex. 2024, "Quantum Technology Monitor 2024," McKinsey, https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/steady%20progress%20in%20approaching%20the%20quantum%20advantage/quantum-technology-monitor-april-2024.pdf. .
[26] Schmaltz, Thomas, Endo, Chie, Eßwein, Robin, Groth, Juliane, Gruber, Sonia, Kroll, Henning, Vogelsang, Manuel M., Neuhäusler, Peter, and Weymann, Lukas, 2025, "Quantentechnologien und Quanten-Ökosysteme," Fraunhofer ISI, https://www.e-fi.de/fileadmin/Assets/Studien/2025/StuDIS_07_2025_.pdf.

leading academic institutions in the US.[27] Overall, European institutions rank highly among globally competitive research institutions (along with the UK, Canada and Australia).[28]

Patent outputs and published developments suggest that China is currently the global leader in quantum communications.[29] Assessments of leadership in sensing and computing fluctuate based on source and methodology, with neither the US nor China enjoying clear dominance over publications, patents and breakthroughs. According to a 2025 OECD report, the US leads in computing and is competitive in sensing; other observers consider recent Chinese developments to match the achievements of US big tech in quantum computing.[30] While Europe does not have a sector-specific patent dominance, the McKinsey analysis (mentioned above) found that Europe accounts for 44 percent of quantum-related patents *awarded* in 2000-2023, despite only accounting for 20 percent of global *requests*.[31] This indicates a high level of quality of the patent requests submitted, pointing to the strength of the underlying research and talent. Specifically, French and German researchers and companies account for nearly a quarter of all quantum-related patents granted during this period, although some of the big contributors are ultimately not controlled from within the EU, despite being located in Europe (for example, IBM Deutschland or Huawei's German subsidiary in Düsseldorf).[32]

Practical Application: Private Enterprise and State-led Action

As outlined in previous sections, quantum technologies have not yet reached broad maturity. Their adoption will depend on further research advances and will likely occur on varied, application-dependent timelines. Healthcare is the largest commercial market for quantum sensing, including biosensing, bioimaging and spectroscopy of biomaterials, followed by navigation for the automotive sector.[33] There have also been attempts to commercialize quantum encryption networks for companies with secure systems (banks, for example); these networks are expected to gain credibility and traction over time.

To what extent quantum technology will result in viable business use cases is, however, uncertain for many industries, given challenges regarding its integration with existing infrastructure (like the digital cloud and big data), current cost-benefit ratio, accessibility and still-limited understanding of the technology.[34] Many private investors are therefore hesitant to invest in far-off returns of quantum technologies. Computing overall takes the main focus of commercial quantum ventures globally, while communications and sensing startups

---

[27] Wong Leung, Jennifer, Robin, Stephan, and Cave, Danielle, 2024, "ASPI's Two-Decade Critical Technology Tracker: The Rewards of Long-Term Research Investment," Australian Strategic Policy Institute, https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2024-08/ASPIs%20two-decade%20Critical%20Technology%20Tracker_1.pdf?VersionId=1p.Rx9MIuZyK5A5w1SDKIpE2EGNB_H8r.
[28] Parker, Edward, Silberglitt, Richard, Gonzales, Daniel, Henrique Sanchez, Natalia, Lee, Justin W., Rand, Lindsay, Schmid, Jon, Dortmans, Peter, Eusebi, Christopher A., 2023, "An Assessment of U.S.-Allied Nations' Industrial Bases in Quantum Technology," RAND Corporation, https://www.rand.org/pubs/research_reports/RRA2055-1.html.
[29] Hmaidi, Antonia and Groenewegen-Lau, Jeroen, 2024, "China's Long View on Quantum Tech Has the US and EU Playing Catch-Up," Mercator Institute for China Studies, https://merics.org/en/report/chinas-long-view-quantum-tech-has-us-and-eu-playing-catch; OECD, 2025, "A Quantum Technologies Policy Primer."
[30] OECD, 2025, "A Quantum Technologies Policy Primer."; Romero, Luis E., 2025 "Quantum Singularity Ahead? China's Zuchongzhi-3 Reshapes Quantum Race," *Forbes*, March 10, 2025, https://www.forbes.com/sites/luisromero/2025/03/10/quantum-singularity-ahead-chinas-zuchongzhi-3-reshapes-quantum-race/.
[31] Bogobowicz et al., 2024, "Quantum Technology Monitor 2024."
[32] Bogobowicz et al., 2024, "Quantum Technology Monitor 2024."; European Commission and European Investment Bank, 2024, "A Quantum Leap in Finance: How to Boost Europe's Quantum Technology Industry," https://data.europa.eu/doi/10.2867/297484.
[33] Settelen, Michael, Venegas-Gomez, Purohit, Abhishek, and Amstrong, Simon, 2024, "Quantum technology: Quantum Sensing Applications in Healthcare," in *Reverse Dependency: Making Europe's Digital Technological Strengths Indispensable to China*, ed. Tim Rühlig, Digital Power China, 59—75, https://dgap.org/system/files/article_pdfs/DPC%20-%20GESAMT_Final.pdf.
[34] Batra, Gaurav, Gschwendtner, Martina, Ostojic, Ivan, Queirolo, Andrea, Soller, Henning, and Wester, Linde, 2021, "Shaping the Long Race in Quantum Technologies," McKinsey, https://www.mckinsey.com/industries/industrials-and-electronics/our-insights/shaping-the-long-race-in-quantum-communication-and-quantum-sensing.

account for a smaller fraction of the ecosystem.[35] There has been a 43 percent drop in quantum startups worldwide between 2022 and 2023; instead, 70 percent of venture capital funding went to scaling up established companies.[36] Overall, US-based investors accounted for €2.3 billion of a global total of €6 billion in venture capital investment between 2012 and 2024, with their EU-based counterparts investing €1 billion.[37] Similarly, public initiatives and funding, which currently constitute the most important pieces of the puzzle in the global quantum landscape's development (€36 billion in the period from 2012 to 2024) play out differently across the US, China and Europe.[38]

United States

The US is the only country that has managed to establish itself as a genuine hub for quantum startups, where private investment matches that provided by the public sector.[39] Its vibrant startup landscape features several later-stage startups, which are more resilient to investor aversion to new technologies just emerging from the research stage.[40] Big tech companies like Microsoft, IBM and Google also host leading quantum computing and hardware efforts.

The emergence of a private US quantum industry has been closely associated with state-driven endeavors.

The centrality of US private enterprise aside, startups typically spin out of academic institutions and continue those partnerships for research, thus continually benefiting from public support.[41] A national focus on public and defense applications has led to procurement of early-stage quantum computers to investigate their implementations in government, army and ministries.[42] The emergence of a private US quantum industry has thus been closely associated with state-driven endeavors, such as the US National Quantum Initiative, which first focused on research and development expansion in 2018. Such efforts laid the foundation for later steps, including the new, industry-backed $2.5 billion *Quantum Leadership Act* to address supply chain challenges and increase commercialization until 2030,[43] or the targeted quantum sensing improvement program for accelerated deployment in the military.[44]

China

Compared to the US, China relies less on private investors in an environment shaped by public initiatives. China's quantum development is rooted in an extensive network of state-aligned academic and commercial institutions that pursue outright collaborative efforts and investments in favor of an independent technology ecosystem.[45] Like the US, China has developed a national strategy to spur initiatives that maintain its competitive edges in quantum subfields and directs public funding to applications with national security and economic growth opportunities. Notable focus areas include superconducting computing and

---

[35] Bogobowicz et al., 2024, "Quantum Technology Monitor 2024."
[36] Bogobowicz et al., 2024, "Quantum Technology Monitor 2024."
[37] Cerutti, Isabella, Di Girolamo, Francesca, Martinze Cillero, Maria, Nardo, Michela, Scudo, Petra, and Zaurino, Elena, 2025, "EU role in the global quantum race," https://publications.jrc.ec.europa.eu/repository/handle/JRC142902.
[38] Cerutti et al., 2025, "EU role in the global quantum race."
[39] Bogobowicz et al., 2024, "Quantum Technology Monitor 2024."
[40] Bogobowicz et al., 2024, "Quantum Technology Monitor 2024." European Commission and European Investment Bank, 2024, "A Quantum Leap in Finance: How to Boost Europe's Quantum Technology Industry."
[41] Bogobowicz et al., 2024, "Quantum Technology Monitor 2024."; OECD, 2025, "A Quantum Technologies Policy Primer."
[42] Küsters, 2025, "Von Superposition Zu Superstrategie?"
[43] Swayne, Matt, 2025, "Senators Introduce $2.5 Billion Bill to Expand U.S. Quantum Research," *The Quantum Insider,* February 14, 2025, https://thequantuminsider.com/2025/02/14/senators-introduce-2-5-billion-bill-to-expand-u-s-quantum-research/.
[44] DARPA, 2025, "Taking Quantum Sensors out of the Lab and into Defense Platforms," accessed June 7, 2025, https://www.darpa.mil/news/2025/quantum-sensors-defense-platforms.
[45] European Quantum Industry Consortium, 2025, "A Portrait of The Global Patent Landscape in Quantum Technologies," https://www.euroquic.org/wp-content/uploads/2025/02/A-Portrait-of-The-Global-Patent-Landscape-in-Quantum-Technologies-2025.pdf.

quantum-satellite communications.[46] While estimates of Chinese public investment in quantum range widely (from $4 billion to $17 billion), they are clearly substantial.[47] Chinese public procurement contracts also go exclusively to national companies; this is in comparison to 70 percent in the US and 12 percent in the EU.[48]

Europe

In contrast to the US and China, Europe has so far struggled to convert academic prowess in quantum technologies into practical, real-world applications for deployment. (The United Kingdom somewhat differs from the continent with a vibrant ecosystem of investors attracted to companies spinning out of heavily funded, reputable research institutions in Oxford, Cambridge and London, e.g., Quantinuum, originally Cambridge Quantum.[49]) But it is not for lack of investment: the EU made the largest announced public investment in the field, with a cumulative €11 billion to date, sourced from both national and EU-wide initiatives.[50] With its "Quantum Flagship" program, launched in 2018, the EU has made a decade-long commitment to the tune of €1 billion to fund targeted projects that enhance national domestic capabilities in quantum technologies – all with the aim to create a diversified research portfolio, but without specific emphasis on commercialization or state-led practical use in areas such as defense.[51]

Europe has so far struggled to convert academic prowess in quantum technologies into practical, real-world applications for deployment.

EU funding has contributed to over 80 research projects, from building quantum biotech simulations to analyzing infrastructure for scalable sensing architectures.[52] In some ways, these projects echo US and Chinese developments on a smaller scale, including efforts to integrate quantum computers into federal institutions and to implement QKD networks.[53] The EU has also launched a procurement initiative for EU-native quantum computers, aiming to distribute them across public institutions to enable broad academic access.[54]

Within the EU, Germany is the primary European quantum hub, followed by France and Finland. Each country is aiming to develop its own, publicly funded quantum computers within the next ten years.[55] Overall, the EU is home to around one third of global quantum

---

[46] De Luca, Stefano, Reichert, Jasmin, 2024, "Quantum: What Is It and Where Does the EU Stand?," European Parliament Research Service, https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/760413/EPRS_ATA(2024)760413_EN.pdf; Hmaidi and Groenewegen-Lau, 2024, "China's Long View on Quantum Tech."
[47] OECD, 2025, "A Quantum Technologies Policy Primer."
[48] Küsters, 2025, "Von Superposition Zu Superstrategie?"
[49] Wheeler, Kitty, 2024, "Why the UK Is World Leading for Quantum Companies," *Technology Magazine*, November 1, 2024, https://technologymagazine.com/articles/why-the-uk-is-world-leading-for-quantum-companies; UKQuantum, 2024, "UK Recognised as World Leading For Creating Quantum Companies And Attracting Investment," accessed May 23, 2025, https://ukquantum.org/uk-recognised-as-world-leading-for-creating-quantum-companies-and-attracting-investment/.
[50] European Commission, 2025, "Quantum Europe Strategy: Quantum Europe in a Changing World, https://digital-strategy.ec.europa.eu/en/library/quantum-europe-strategy.
[51] European Commission, 2025, "Quantum: Shaping Europe's Digital Future," accessed June 5, 2025, https://digital-strategy.ec.europa.eu/en/policies/quantum.
[52] Abdi, Ismail, Dugo, Andrea, Erixon, Fredrik, and Tähtinen, Lauri, 2025, "The 8 Percent Approach: A Big Bang in Resources and Capacity for Europe's Economy and Defence," European Centre for International Political Economy, https://ecipe.org/wp-content/uploads/2025/02/ECI_OccasionalPaper_02-2025_LY06.pdf; De Luca and Reichert, 2024, "Quantum: What Is It and Where Does the EU Stand?"
[53]Erixon, Fredrik, Dugo, Andrea, Pandya, Dyuti, and du Roy, Oscar, 2025, "Benchmarking Quantum Technology Performance: Governments, Industry, Academia and Their Role in Shaping Our Technological Future," European Centre for International Political Economy, https://ecipe.org/publications/benchmarking-quantum-technology-performance/. OECD, 2025, "A Quantum Technologies Policy Primer."
[54] European Commission and European Investment Bank, 2024, "A Quantum Leap in Finance: How to Boost Europe's Quantum Technology Industry."
[55] Parker et al., 2023, "An Assessment of U.S.-Allied Nations' Industrial Bases in Quantum Technology."; Weber, Valentin and Pericàs Riera, Maria, 2025, "Quantum Technologies: Ranking Germany's Ambition and International Reputation," German Council on Foreign Relations, https://dgap.org/system/files/article_pdfs/10_DGAP%20Policy%20Brief%202025_EN_Quantum_Tech_0.pdf.

companies, though most of them are smaller and younger compared to counterparts in the US and China.[56] French company Pasqal and Finland's IQM are examples of promising private quantum startups in the nascent field of computing technologies.[57]

Fundamentally, however, driving a coherent effort toward clear, strategic outcomes has proven challenging in the EU's multi-level system. In part, this is due to the relatively early stage of technology development as well as the sheer diversity of the quantum stack. Both factors make it challenging to anticipate specific development pathways and achieve coordinated action in a complex political and institutional setup like the EU.

On the other hand, Europe does benefit from strengths in adjacent, more mature technologies that can be used to support quantum tech. A prime example of this would be the case of semiconductor hardware and specialized control equipment manufacturing, which is the main commercially ready layer of the quantum stack on the continent.[58] The Dutch company ASML has an 80 percent market share in semiconductor machinery production, which is also vital for quantum technologies.[59]

According to a 2024 analysis by the European Investment Bank, the continent suffers from a lack of active, specialized technology investors, which also drives a perception among global, generalist investors that small-scale European technology companies come with high risks and only limited promise.[60] Europe's lack of private investment in quantum technology has led to a brain drain of sorts, where commercially promising ventures, talent and intellectual property are pulled away mainly to the US (which accounts for 44 percent of global private investment in quantum).[61] While Europe's intellectual prowess in quantum research is undeniable, the continent has hardly been able to capitalize on these strengths.

Brussels has started to work on a more comprehensive and ambitious approach in conjunction with its 2023 Economic Security Strategy.

In the last years, Brussels has started to work on a more comprehensive and ambitious approach in conjunction with its 2023 Economic Security Strategy. This includes its decision to earmark quantum technologies as a focus area for technology security risks and leakage. The recognition that quantum technologies have the potential to enhance military and intelligence capabilities is also driving an ongoing risk assessment of potential controls on quantum-related exports and outbound investment .[62]

Moreover, the EU just released the Quantum Europe Strategy in July 2025.[63] The new strategy focuses on five priority areas: research and innovation, infrastructure, ecosystem scale-up, space and dual-use applications and quantum skills. It proposes an extensive set of 26 actions across these interconnected aspects, including plans to launch a pilot facility for the European Quantum Internet, establish a quantum design facility and several quantum chips pilot lines, develop a quantum sensing space and defense technology roadmap, and set up a European Quantum Skills Academy. The strategy will be followed by a *Quantum Act* in 2026, intended to further strengthen Europe's response to economic and security challenges related to the emergence of quantum technologies. Together, both are hoped to pool resources, coordinate

---

[56] Cerutti et al., 2025, "EU role in the global quantum race."
[57] Bogobowicz et al., 2024, "Quantum Technology Monitor 2024."
[58] Bogobowicz et al., 2024, "Quantum Technology Monitor 2024."
[59] Kleinhans, Jan-Peter and Lee, John, 2024, "Is the EU's Semiconductor Manufacturing Equipment a Strategic Chokepoint?", in *Reverse Dependency: Making Europe's Digital Technological Strengths Indispensable to China*, ed. Tim Rühlig, Digital Power China, 30—43, https://dgap.org/system/files/article_pdfs/DPC%20-%20GESAMT_Final.pdf.
[60] European Commission and European Investment Bank, 2024, "A Quantum Leap in Finance: How to Boost Europe's Quantum Technology Industry."
[61] Erixon et al., 2025, "Benchmarking Quantum Technology Performance."
[62] European Commission, 2025, "Commission Recommendation (EU) 2025/63 of 15 January 2025 on Reviewing Outbound Investments in Technology Areas Critical for the Economic Security of the Union," https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202500063.
[63] European Commission, 2025, "Quantum Europe Strategy: Quantum Europe in a Changing World."

research investments and "foster a resilient, sovereign quantum ecosystem", making "Europe a global leader in quantum by 2030."[64]

While these recent steps are encouraging in terms of advancing the EU quantum ecosystem in general, it will remain important to dedicate close attention to the issues quantum technologies pose specifically from a security perspective and to prioritize measures accordingly.

Security Considerations from a European Vantage Point

Across the quantum subfields, technical innovation has implications for (1) dual-use and military applications, (2) cybersecurity and critical data protection and (3) exposure to supply chain vulnerabilities and economic coercion.

Table 1. Key security considerations across quantum subfields.

	Communications	Sensing	Computing
Military & Dual-Use	Dual-use global encryption networks, with interconnected sensing systems	Discrete navigation and enhanced surveillance Precise target detection Biosensing for human enhancement	Accelerated development of (bio-) weapons, neurotech and medical tech Support for complex military logistics & decision-making
Cybersecurity & Data	Cryptography research for attack prevention also enabling development of novel attack algorithms Non-uniform global cryptography standards forcing continuous adaptation to adversary developments	Detection and exploitation of minute hardware vulnerabilities in critical systems	More powerful cyberattacks on critical systems Mass decryption of global intelligence, private and personal data Data hoarding ("Harvest now, decrypt later")
Technology Availability & Coercion Risks	Often niche, multidisciplinary quantum applications with yet indetermined supply chains Difficulty in gaining value, indispensability and talent within US-China-dominated global ecosystem Risk of coercive withholding of technology access		

[64] European Commission, 2025, "Commission launches strategy to make Europe Quantum leader by 2030," accessed July 3, 2025, https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1682; European Commission, 2025, "Commission Work Programme 2025, Moving Forward Together: A Bolder, Simpler, Faster Union," accessed May 11, 2025, https://commission.europa.eu/strategy-and-policy/strategy-documents/commission-work-programme/commission-work-programme-2025_en.

The US and China – relatively early in recognizing many of these concerns – have embraced a security-centric approach to quantum innovation, including expanding export controls and setting up collaboration restrictions.[65] Against this backdrop, other governments have embraced the pursuit of "quantum sovereignty." Table 1 provides an overview of key security considerations in each of the three subfields; these considerations are expanded upon in the following paragraphs.

Military and Dual-Use

Quantum technologies have clear military applications; indeed, they hold the potential to create a new domain of warfare, with unique advances in undetectable navigation and reconnaissance, secure intelligence and precise target acquisition. Near-term sensing and communications systems provide independent, covert and encrypted military intelligence capabilities. For example, the US, in cooperation with quantum AI company SandboxAQ, has developed a submarine and air navigation system that is completely satellite-independent[66] and has quantum sensors that are continuously monitoring its positioning and any interfering electromagnetic and gravitational forces.[67] Precise reconnaissance and target detection from quantum sensors can enable surveillance through underground or underwater infrastructure and thereby enable the use of other weapons systems such as missiles or drones.[68] China was the first to establish a mobile QKD network that spans over 4600 km[69] and transmits encrypted data between drones and satellites;[70] the US and the EU are both attempting to replicate this system.[71]

Both the US and China are trying to leverage international partnerships with military or dual-use dimensions to quantum technologies. AUKUS (the trilateral military alliance between Australia, the UK and the US), for example, is attempting to widen the gap with China in military quantum sensing.[72] BRICS partners, on the other hand, stand to benefit from Chinese advancements in quantum communications; Russia and South Africa have partnerships to expand the Chinese quantum network to span 12,900 km.[73]

In addition, there are dual-use risks associated with quantum sensing and computing-enabled biotechnology. Quantum simulations can provide insights into molecular interactions and

---

[65] Brooke-Holland, Louisa, 2024, "AUKUS Pillar 2: Advanced Military Capabilities," House of Commons Library, https://securityanddefenceplus.plusalliance.org/wp-content/uploads/2024/05/AUKUS-Pillar-2-Advanced-Capabilities-Research-Briefing-%E2%80%93-House-of-Commons-Library.pdf; Erixon et al., 2025, "Benchmarking Quantum Technology Performance."; Küsters, 2025, "Von Superposition Zu Superstrategie?"; Okano-Heijmans, Maaike, Gomes, Alexandre, and Dekker, Brigitte, 2024, "Balancing Openness, Economic Security and National Security: The Future of Export Controls on Quantum Technologies," Clingendael, https://www.clingendael.org/sites/default/files/2024-04/Clingendael_report_The_future_of_export_controls_on_quantum_technologie.pdf.

[66] Krelina, Michal. 2025, "An Introduction to Military Quantum Technology for Policymakers," Stockholm International Peace Research Institute, https://www.sipri.org/sites/default/files/2025-03/2025_03_quantum_1.pdf.

[67] SandboxAQ, 2024 "SandboxAQ Completes Major AQNav Milestones with the USAF," accessed April 16, 2024, https://www.sandboxaq.com/post/sandboxaq-completes-major-aqnav-milestones-with-the-usaf.

[68] OECD, 2025, "A Quantum Technologies Policy Primer."

[69] Chen, Y., Zhang, Q., Chen, T., Cai, W., Liao, S., Zhang, J., Chen, K., Yin, J., Ren, J., Chen, Z., Han, S., Yu, Q., Liang, K., Zhou, F., Yuan, X., Zhao, M., Wang, T., Jiang, X., Zhang, L., Liu, W., Li, Y., Shen, Q., Cao, Y., Lu, C., Pan, J., 2021, "An Integrated Space-to-Ground Quantum Communication Network over 4,600 Kilometres," *Nature* 589, pp. 214—19, https://doi.org/10.1038/s41586-020-03093-8.

[70] Tian, X., Yang, R., Liu, H., Fan, P., Zhang, J., Gu, C., Chen, M., Hu, M., Lu, F., Zhu, C., Yin, Z., Yin, Z., Yuan, M., Wang, S., Chen, W., Gong, Y., Zhu, S., and Xie, Z., 2024, "Experimental Demonstration of Drone-Based Quantum Key Distribution," *Physical Review Letters* 133, 200801, https://doi.org/10.1103/PhysRevLett.133.200801.

[71] European Quantum Flagship and European Commission, 2024, "SRIA 2030: Roadmap and Quantum Ambitions over This Decade," https://qt.eu/media/pdf/Strategic-Reseach-and-Industry-Agenda-2030.pdf?m=1707900786&.

[72] Brooke-Holland, 2024, "AUKUS Pillar 2."

[73] Swayne, Matt, 2025, "China Establishes Quantum-Secure Communication Links With South Africa," *The Quantum Insider*, March 14, 2025, https://thequantuminsider.com/2025/03/14/china-established-quantum-secure-communication-links-with-south-africa/.

accelerate the development of precision medicine. When used for nefarious purposes, this technology can be part of the development of targeted biological weaponry, neurotechnology and human enhancement for defense applications.[74] These dual-use risks intersect with concerns relating to cyber and economic security, discussed below.

A general complication regarding military and dual-use applications is that various (potentially impactful) devices are conceivable without depending on the overall advancement toward FTQC. Unique development pathways for these devices make the risk landscape even more complex and dynamic. For example, the communications field of "quantum radar," in which promising devices are based on photonic systems, remains underdeveloped.[75] However, simultaneous developments in quantum chemistry and materials simulations could create photonic-resistant coatings for stealth instruments.[76] It is therefore uncertain to what extent this technology can provide a relevant edge and warrants significant investment (without a clear pathway to sure-fire results).

The EU's Quantum Europe Strategy recognizes quantum technology's dual-use dimension and acknowledges its integral role in ensuring Europe's security and techno-economic sovereignty.[77] It promises to accelerate the uptake of civil quantum innovations into security and defense applications and to shorten development cycles to reinforce Europe's technological edge in capabilities with dual-use potential. Promised roadmaps for quantum technology applications in space and defense now need to bring clarity on what the EU aims to achieve in the realm of quantum technologies for military and defense, for example, in terms of combining national capabilities with those accessible through NATO (particularly, those of the US, UK and Canada). There is also an emerging debate on forming a coalition of individual European quantum tech powers (Germany, the Netherlands and France) to potentially streamline multilateral discussions instead of trying to align engagement from all the EU member states.[78] Accordingly, member states, too, need to reflect on their objectives regarding quantum technology's military applications.

A critical ingredient will be a deeper and more systematic assessment of threats and opportunities in the military domain, given considerable uncertainty about the future technology pathway and the practical utility of innovations for the battlefield and beyond. Based on a clear shared perspective, stakeholders (including research institutions and European startups) could explore possible public-private defense partnerships, as well as working towards a more security-minded approach to innovation and risk management across the ecosystem.

Cybersecurity and Data Protection

There are several ways quantum technologies could undermine the very foundations of the current global data security architecture. Firstly, quantum sensors can monitor micro-interactions from existing technologies, opening the door to novel hacking techniques through deductions on the workings of critical infrastructure (for example, financial or nuclear systems).[79] International quantum networks may also be used to spy, sabotage or violate data privacy in an imperceptible manner; examples include the weaponization of

---

[74] Fu, K. , Greiner, M., Hazzard, K., Hulet, R., Kollár, A., Lev, B., Lukin, M., Ma, R., Xiao, M., Misra, S., Monroe, C., Murch, K., Nazario, Z., Ni, K., Potter, A., Roushan, P., Saffman, M., Schleier-Smith, M., Siddiqi, I., Simmonds, R., Singh, M., Spielman, I., Temme1, K., Weiss, D., Vučković, J., Vuletić, V., Ye, J., and Zwierlein, M., 2021, "Quantum Simulators: Architectures and Opportunities," *PRX Quantum* 2, no. 017003, https://doi.org/10.1103/PRXQuantum.2.017003.
[75] Karsa, A., Fletcher, A., Spedalieri, G., and Pirandola, S. 2024, "Quantum Illumination and Quantum Radar: A Brief Overview," *Reports on Progress in Physics* 87, no. 9, 094001, https://doi.org/10.1088/1361-6633/ad6279.
[76] Krelina, 2025, "An Introduction to Military Quantum Technology for Policymakers."
[77] European Commission, 2025, "Quantum Europe Strategy: Quantum Europe in a Changing World."
[78] Okano-Heijmans, Gomes, and Dekker, 2024, "Balancing Openness, Economic Security and National Security."
[79] Cyberagentur, 2025, "Side-Channel Attacks with Quantum Sensing (SCA-QS)," accessed April 14, 2025, https://www.cyberagentur.de/en/programs/sca-qs/.

commercial components or (ab)using vulnerabilities in hardware or interconnects (comparable to the discussion around 5G mobile networks).[80] Breakthroughs in FTQC carry the risk of high-power cyber-attacks, which would be faster than any supercomputer and could build on adversary knowledge gleaned from surveilling sensors and networks.

There are several ways quantum technologies could undermine the current global data security architecture.

Secondly, FTQC threatens the current "public key" encryption approach, which is crucial to maintaining secure systems like secure browsing, financial transactions and communication between government ministries. This approach involves the combination of a secret encryption key and a mathematically related public key. Its security relies on the inability of classical computers to solve the key pair's relationship efficiently, if at all.[81] FTQC algorithms, however, have been mathematically proven to solve these public key relationships using a fraction of the operations non-quantum computers would need, also compromising intermediate authentication codes within various classical encryption protocols.[82]

Adversarial usage of FTQCs could thus expose – *en masse* – national intelligence systems, citizens' personal information and financial data. While this capability is not yet available in practice, adversaries may be hoarding existing data for decryption whenever an FTQC device is developed.[83] China is suspected to have harvested encrypted data on a large scale in 2016-2017, when its intelligence services covertly intercepted six months of internet traffic from Canada to Korea, as well as several interceptions within Europe and Asia.[84] Russia has similarly siphoned data from Google, Facebook and Amazon networks in 2019 and all internet traffic passing through the occupied regions of Ukraine in 2022.[85] Given the significant computing resources needed for quantum cyberattacks, nation states (rather than individuals or non-state groups) are the greatest threat to classical encryption systems.[86]

Post-quantum cryptography (PQC) seeks to counter this threat by developing and implementing new classical encryption methods that are resistant to such FTQC attacks. The research into the workings and faults of cryptographic algorithms ("cryptanalysis") is inherently dual use. The US is the most advanced in adopting PQC, having formally established quantum cryptography as a threat to national security in 2022.[87] The National Institute of Standards and Technology (NIST) has since produced three finalized PQC standards and has granted public support to help US organizations transition to PQC.[88] The EU and G7 member states have similarly acknowledged the necessity of PQC for financial and private data

---

[80] Krause, Juljan, 2021, "The Quantum Threat: Why We Need Regulation and Transparency," *about:intel: European Voices on Surveillance*, February 8, 2021, https://aboutintel.eu/quantum-threat/.; OECD, 2025, "A Quantum Technologies Policy Primer."; Soller et al., 2025, "Quantum Communication: Trends and Outlook."

[81] Gitonga, C. 2025 "The Impact of Quantum Computing on Cryptographic Systems: Urgency of Quantum-Resistant Algorithms and Practical Applications in Cryptography," European Journal of Information Technologies and Computer Science 5, no. 1, pp. 1—10, https://doi.org/10.24018/compute.2025.5.1.146.

[82] Krelina, 2021, "Quantum Technology for Military Applications."

[83] OECD, 2025, "A Quantum Technologies Policy Primer."

[84] Demchak, C. and Shavitt, Y., 2018, "China's Maxim – Leave No Access Point Unexploited: The Hidden Story of China Telecom's BGP Hijacking," *Military Cyber Affairs* 3, no. 1, https://doi.org/10.5038/2378-0789.3.1.1050.

[85] Doffman, Zak, 2022, "Russia And China 'Hijack' Your Internet Traffic: Here's What You Do," *Forbes*, April 18, 2020, https://www.forbes.com/sites/zakdoffman/2020/04/18/russia-and-china-behind-internet-hijack-risk-heres-how-to-check-youre-now-secure/; Reuters, 2022, "Russia Reroutes Internet Traffic in Occupied Ukraine to Its Infrastructure," May 2, 2022, https://www.reuters.com/world/europe/russia-reroutes-internet-traffic-occupied-ukraine-its-infrastructure-2022-05-02/.

[86] Mohammad Alhammouri, Shah, Ahmad, Qamar, Ismail, and Qureshi, Ali, 2025, "Securing Data in the Post-Quantum Age," PwC, accessed April 16, 2025, https://www.pwc.com/m1/en/publications/securing-data-in-the-post-quantum-age.html.

[87] White House, 2022, "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems," accessed May 5, 2025, https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/.

[88] Information Technology Laboratory Computer Security Division, 2017, "Post-Quantum Cryptography (PQC)," NIST, accessed May 5, 2025, https://www.nist.gov/pqcrypto.

protection; full implementation of PQC is in the planning stage[89] and most countries expect to use NIST standards within the next five years.[90] China, meanwhile, has pursued its own initiative, diverging from the US. Mutual distrust between the US and China is preventing the establishment of any unified standard, as each suspects the other of potential betrayal or non-compliance.[91]

This parallel, non-unified PQC development may result in the discovery of new quantum decryption algorithms.[92] It could also contribute to the emergence of multiple separate, more state-controlled quantum internets, which would arguably suit the agenda of authoritarian governments.[93] Finally, PQC implementation to secure all sensitive data platforms is expected to take extensive time, financial resources and research.[94]

Immediate action and investment in PQC are necessary to establish a robust cybersecurity solution and face future quantum computing capabilities. The European Commission has set up a PQC workstream led by France, Germany and the Netherlands, which is currently coordinating the EU-wide adoption of standards and subsequent migration of systems and their data.[95] Because of the cost and implementation effort, the workstream advocates for a "hybrid" migration strategy that prioritizes key systems for national security and financial institutions.

The Commission followed up with a Roadmap for the Transition to Post-Quantum Cryptography in June 2025, providing some clarification with regards to implementation methodology and timelines. Further specification and sustained commitment to driving implementation are necessary to ensure that critical systems are not left temporarily vulnerable in the process. Moreover, dedicated research seems warranted to develop reliable cybersecurity safeguards that can be more easily deployed for lower priority systems. Similarly, regarding the issue of harvested data, further research is needed to evaluate data that has already (potentially) been exposed, its scale and its criticality; intermediary methods of mitigation to secure vulnerable data networks in the meantime, must also be investigated.

Availability of Technology and Coercion Risks

Many quantum devices are geared toward rather niche applications. Therefore, it seems unlikely for a quantum industry as such to reach huge proportions in any economy, even as the market is projected to grow significantly in the coming decades.[96] In the case of a major FTQC breakthrough, quantum communications and cybersecurity tools and services will have the broadest applicability across various sectors with data-transmission use-cases. More widespread use of quantum computing in complex science, finance and machine learning is also possible, but the current consensus is that traditional computers will typically remain the preferred option – at least until the cost-benefit advantage of quantum alternatives becomes

[89] OECD, 2025, "A Quantum Technologies Policy Primer."
[90] GSMA, 2025 "Post Quantum Government Initiatives by Country and Region," accessed May 6, 2025, https://www.gsma.com/newsroom/post-quantum-government-initiatives-by-country-and-region/.
[91] Matt Swayne, 2025, "China Launches Its Own Quantum-Resistant Encryption Standards, Bypassing US Efforts," *The Quantum Insider*, February 18, 2025, https://thequantuminsider.com/2025/02/18/china-launches-its-own-quantum-resistant-encryption-standard-bypassing-us-efforts/.
[92] OECD, 2025, "A Quantum Technologies Policy Primer."
[93] Juljan Krause, 2021, "The Quantum Threat."
[94] Gitonga, 2025, "The Impact of Quantum Computing on Cryptographic Systems"; Krelina, 2021, "Quantum Technology for Military Applications."; OECD, 2025, "A Quantum Technologies Policy Primer."; Soller et al., 2025, "Quantum Communication: Trends and Outlook."
[95] Dutch Ministry of Security and Justice , German Federal Office for Information Security, and French National Agency for the Security of Information Systems, 2024, "Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography," https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement.pdf?__blob=publicationFile&v=5.
[96] Bogobowicz et al., 2024, "Quantum Technology Monitor 2024."

more compelling than is currently anticipated.[97] Still, a reliance on emerging devices and techniques in critical domains can pose economic security challenges, notably in terms of access to raw materials, inputs and talent.

Quantum technologies fundamentally draw upon a variety of sectors, and each technology requires different raw materials and engineering methods for its development. The cross-sectoral nature of these technologies means that quantum tech's critical dependencies range widely, intersecting with semiconductor, AI, pharmaceutical, chemical and aerospace supply chains. The rapidly changing state of device architecture makes it difficult to pinpoint emerging critical dependencies or to strategically intervene in the ecosystem to drive innovation.[98] For example, superconducting computers are promising in the computing space but require novel 3D manufacturing approaches for large-scale use.[99] In contrast, photonic chips could be manufactured in conventional factories, and may become more efficient in the long term.[100]

Raw materials are a likely candidate for supply chain disruption, followed by assembly equipment and technical expertise.

Preliminary research from the US Quantum Economic Development Consortium found that US industry sees key raw materials as the most likely candidate to wreak supply chain disruption, followed by assembly equipment, and then technical expertise.[101] US-China export controls – specifically targeting materials and components used for quantum tech – point to a similar thinking. To date, US export controls have been put in place to limit, among other things, cryogenic control equipment for superconducting computing, microfabricated silicon and germanium used for spin-based computers, and the acquisition of entire US-origin quantum computers.[102] China, similarly placed export controls on key rare earth metals that may be necessary for end-stage quantum devices, such as neodymium and yttrium, leveraging its leading position in the supply of these materials.[103]

In the computing field, a somewhat unusual source of influence and leverage could be the lack of widely accepted benchmarking, which makes it difficult to distinguish genuine from misleading advancements and hinders investors in allocating resources to the most promising initiatives. The US is currently the only nation with a quantum benchmarking initiative (QBI) to evaluate all computing architectures. The QBI and the US Defense Advanced Research Projects Agency (DARPA) intend to fund promising companies, with the goal of US government procurement of a utility-scale quantum computer by 2033.[104] Private companies in the US, Canada, Australia, the UK and the EU have been offered this funding to accelerate their development. As the only initiative of its kind, QBI will play a key role in setting market expectations for quantum computing companies. This could conceivably create an advantage

---

[97] Batra et al., 2021, "Shaping the Long Race in Quantum Technologies."; Moskvitch, Kate, 2025, "What Is 'quantum Advantage' and How Can Businesses Benefit from It?," World Economic Forum, accessed May 15, https://www.weforum.org/stories/2025/04/quantum-computing-benefit-businesses/.
[98] Sorensen, Bob and Sorensen, Tom, 2022, "Challenges and Opportunities for Securing a Robust US Quantum Computing Supply Chain", QED-C, https://quantumconsortium.org/publication/quantum-computing-supply-chain-issues/.
[99] Yost, D., Schwartz, M., Mallek, J., Rosenberg, D., Stull, C., Yoder, J., Calusine, G., Cook, M., Das, R., Day, A., Golden, E., Kim, D., Melville, A., Niedzielski, B., Woods, W., Kerman, A., and Oliver, W., 2020, "Solid-State Qubits Integrated with Superconducting through-Silicon Vias," *NPJ Quantum Information* 6, no. 59, pp. 1—7, https://doi.org/10.1038/s41534-020-00289-8.
[100] Küsters, 2025, "Von Superposition Zu Superstrategie?"
[101] Sorensen and Sorensen, 2022, "Challenges and Opportunities for Securing a Robust US Quantum Computing Supply Chain."
[102] Industry and Security Bureau, 2024, "Commerce Control List Additions and Revisions; Implementation of Controls on Advanced Technologies Consistent With Controls Implemented by International Partners," Federal Register, accessed April 16, 2025, https://www.federalregister.gov/documents/2024/09/06/2024-19633/commerce-control-list-additions-and-revisions-implementation-of-controls-on-advanced-technologies.
[103] Quantum Economic Development Consortium (QED-C), 2025, "State of the Global Quantum Industry 2025."; Rogers, Michael S., Zeng, William, Lewis, James A., Rajic, Taylar, and Hill, Jonah, F., 2025, "CSIS Commission on U.S. Quantum Leadership," Center for Strategic and International Studies, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2025-01/250131_Lewis_Quantum_Commission.pdf?VersionId=DD9FIUtCQwWzJAB7kVpJBa2f0sn30Hf9.
[104] DARPA, n.d., "Quantum Benchmarking Initiative," accessed April 14, 2025, https://www.darpa.mil/research/programs/quantum-benchmarking-initiative.

for US players and contribute to a consolidation of US control over the commercial market for quantum computing.

With the US being the global leader in computing-related research and producing twice as many outputs as China, the Australian Strategic Policy Institute has suggested that there is a medium risk of an American monopoly in quantum computing.[105] The US appears committed to using its advantage to categorically restrict China's access to American technology; it has already restricted Chinese collaborations and has broadly classified Chinese quantum computing development as a threat to national security.[106] China, meanwhile, may be able to exert comparable influence in the subfield of quantum communications. Such monopolies could expose Europe to techno-economic coercion.[107]

The EU manufactures critical quantum-supporting components and semiconductor lithography equipment, mostly geared toward the production of photonic lasers, select atomic isotopes, refrigerators and vacuum chambers.[108] Notably, the Dutch firm ASML has a global monopoly over the manufacturing of extreme ultraviolet (EUV) lasers and argon-fluoride immersion tools, both of which are specialized components that may prove useful for quantum chip manufacturing. The EU Quantum Flagship has a dedicated project to determine the potential of EUV lasers in quantum technologies[109] and the associated semiconductor industry.[110] It remains unclear, however, if these devices will ultimately prove a chokepoint in future quantum tech supply chains that Europe could leverage. While Chinese chipmakers have not yet been able to overcome their dependence on European lithography for conventional cutting-edge semiconductors, Chinese lithography tooling will likely catch up eventually, according to research by the Digital Power China (DPC) consortium; Europe's upper hand in lithography will be limited in comparison to China's far-reaching control over raw materials.[111]

Achieving and sustaining positions of "strategic indispensability" should be an important guiding consideration for the EU's efforts to foster homegrown innovation.

Still, the complexity and transience of the emerging ecosystem mean it is unlikely that any individual actor will achieve and sustain complete autarky in quantum technologies. Achieving and sustaining positions of "strategic indispensability" in specific niches at the global level to exert influence and deter coercive action by other powers should therefore be an important guiding consideration for the EU's efforts to foster homegrown innovation. In this vein, it is right that the EU is conducting an EU-wide Quantum Technology Risk Assessment to map supply-chain vulnerabilities, which can guide mitigation measures as well as strategic efforts to build own leverage.

Likewise, a systematic assessment of technical barriers in each of the quantum subfields that overlap with the EU's existing academic strengths should be a first step to enable strategic research investments. Quantum technologies still face fundamental unsolved problems (e.g., regarding quantum memory) that point to avenues for breakthrough research and applications.

---

[105] Wong Leung, Robin, and Cave, 2024, "ASPI's Two-Decade Critical Technology Tracker."
[106] Bureau of Industry and Security, 2025, "Commerce Further Restricts China's Artificial Intelligence and Advanced Computing Capabilities," accessed April 16, 2025, https://www.bis.gov/press-release/commerce-further-restricts-chinas-artificial-intelligence-advanced-computing-capabilities.
[107] Okano-Heijmans, Gomes, and Dekker, 2024, "Balancing Openness, Economic Security and National Security."
[108] Parker et al., 2023, "An Assessment of U.S.-Allied Nations' Industrial Bases in Quantum Technology."
[109] European Quantum Flagship, 2025, "UVQuanT - Deep Ultraviolet Laser For Quantum Technology," accessed April 29, 2025, https://qt.eu/projects/basic-science/uvquant.
[110] PSI Center for Photon Science, 2024, "Extreme Ultraviolet for Scalable Silicon Quantum Devices," accessed May 5, 2025, https://www.psi.ch/en/lsx/scientific-highlights/harnessing-euv-light-for-large-scale-silicon-quantum-device-patterning.
[111] Kleinhans, Jan-Peter and Rühlig, Tim, 2024, "Reverse Dependencies on China: How Europe Can Remain Technologically Indispensable and Preserve its Strategic Autonomy," in *Reverse Dependency: Making Europe's Digital Technological Strengths Indispensable to China*, ed. Tim Rühlig, Digital Power China, 14—29, https://dgap.org/system/files/article_pdfs/DPC%20-%20GESAMT_Final.pdf.

Finally, actively shaping the global regulatory landscape via standardization efforts could help support the spread of EU-origin technologies, though the development or enforcement of standards alone will not make the EU a relevant actor. Considering the example of the US QBI, pursuing an EU benchmarking initiative should serve to ensure that European advances are adequately captured and prized, which may help to retain intellectual and meaningful influence in the market.

Looking ahead

Quantum technologies carry great promise regarding powerful sensors, secure communication and novel solutions to complex computational problems that span various applications, even though significant development is still needed to surpass established non-quantum solutions.

At the same time, the implications of quantum technologies for national and economic security are serious and cannot be dismissed simply because their timeline is uncertain. Countries are increasingly trying to keep pace with global advancements across all the quantum subfields – especially in defense-related applications like quantum sensors and networks or NISQ computers. Within the broader context of the US-China rivalry, each nation's capacity for dual-use innovation or resilience against coercion is being shaped by multilateral partnerships, autonomy-focused national strategies and development-hindering economic controls. In this environment, proactive measures to address pressing risks – such as adopting PQC – should not be delayed until the technical breakthroughs expected have actually materialized.

The EU's primary focus on bolstering quantum innovation has served to maintain its reputation for quantum research and talent. However, to secure a stronger strategic position, it is essential that the EU spurs and supports commercially viable quantum ventures, maintains a consistent stake in the evolving supply and development ecosystem, and ensures resilience from both a defense and economic perspective. The recent release of its Quantum Strategy and PCQ Roadmap demonstrate that Brussels is committed to a comprehensive and ambitious approach regarding quantum-related risks and opportunities. Translating the strategy into real actions and plugging remaining gaps will be critical to safeguard national security, protect data and infrastructure, and direct strategic investments for sustained economic growth and resilience.

Reflect. Advise. Engage.

The Global Public Policy Institute (GPPi) is an independent non-profit think tank based in Berlin. Our mission is to improve global governance through research, policy advice and debate.

Reinhardtstr. 7, 10117 Berlin, Germany
Phone +49 30 275 959 75-0
gppi@gppi.net
gppi.net

GPPi
GLOBAL PUBLIC POLICY INSTITUTE