ITI's Quantum Technologies Policy Principles

and Essentials for Global Policymakers

April 2025

ITI

Promoting Innovation Worldwide

Executive Summary

Quantum Information Science (QIS) represents an evolution in computing and data processing by integrating the principles of quantum mechanics with information science. Innovations in this field have the potential to revolutionize a wide range of industries by leveraging quantum physics for information storage, transmission, computing, or measurement. This technological progress is paralleled by substantial economic potential across a variety of sectors. At the same time, quantum technologies mark a paradigm shift in how organizations think about security as these technologies introduce both new cybersecurity threats and defensive capabilities.

Quantum technologies have profound public policy implications that span national security, economic competitiveness, cybersecurity and data privacy. Accordingly, policymakers are paying close attention due to the disruptive potential offered by these technologies. Countries across the globe see leadership in quantum technologies as an engine for future economic growth and are racing to stake out positions in the emerging quantum enabled economy.

Gaining first mover advantage in quantum technologies – particularly quantum computing – can offer countries and private sector companies significant strategic benefits. However, these strategic advances come with risks, such as high research and development (R&D) costs, supply chain challenges, technology unpredictability and the challenge of building a skilled workforce.

ITI's Quantum Technology Policy Guide is designed to equip policymakers, industry partners, and other stakeholders with foundational knowledge about the current state of quantum technologies, their potential and real-life impacts on global economies, and recommendations on how to nurture the pro-innovation ecosystem necessary for quantum technologies to thrive.

With that in mind, the following globally applicable proposals should be considered:

- **Unleash Innovation and Investments in Quantum Technologies**
- **Support the Development of a Resilient Quantum Technologies Supply Chain**
- **Develop a Skilled Quantum Workforce**
- **Consider the Cybersecurity and Privacy Implications of Quantum Technologies**
- **Adopt a Balanced Approach to Quantum Technologies Governance**
- **Prioritize Global Engagement and Cooperation on Quantum Technologies**

About ITI

As the premier technology trade association with a presence across the globe, ITI represents the full spectrum of technology companies, including those that are contributing to nearly every facet of developing and deploying quantum technologies. Our members understand the complexities of this emerging field and can truly appreciate the potential and real-life impact that these technologies have on the economy.

ITI and our member companies have developed this Quantum Technology Policy Guide as a useful resource for policymakers, industry partners, and other stakeholders looking to both understand this subject matter and explain how governments and industry can work together to develop impactful quantum policies.

The Guide is Divided into Five Sections:

Section I: Quantum Technologies 101 / Page 5

Quantum Technologies 101 provides an introductory overview of the quantum technology landscape. It defines key terms and delineates quantum computing, quantum sensing, and quantum communications.

Section II: Policy Implications of Quantum Technologies / Page 7

Policy Implications of Quantum Technologies studies the application areas in which quantum technologies are poised to drive significant change. This analysis serves as the backdrop for a summary of global policy initiatives that seek to establish their respective countries at the forefront of quantum technology leadership.

Section III: Policy Principles / Page 10

Policy Principles offers six actionable recommendations that support the design of a pro-innovation public policy. Governments should consider developing national strategies that harness academic and private sector innovations that focus on unlocking the benefits for stakeholders across society.

Section IV: Use Cases / Page 16

Use Cases discusses a select number of real-life examples in which quantum technologies have already been deployed with measurable success.

Section V: Glossary / Page 19

Glossary provides an overview of key terms and concepts to inform the reader's understanding of the science and technology underlying quantum.

Section I:
Quantum Technologies 101

Quantum Information Science (QIS) represents an evolution in computing and data processing by integrating the principles of quantum mechanics with information science. Quantum physics studies the unique ways in which (sub-)atomic particles behave. When applied to information science, these unique behaviors and patterns can be leveraged to unlock new information processing paradigms.

Unlike classical bits that are strictly 0s and 1s, quantum bits (qubits) harness quantum properties like superposition and entanglement, enabling exponential leaps in computational power, ultra-secure communications, and unprecedented precision in sensing. There are a number of quantum mechanical systems that potentially could serve as qubits, so called qubit modalities. The term "quantum" itself refers to the discrete quantity of electromagnetic energy proportional in magnitude to the frequency of the radiation it represents.

The field of QIS encompasses a wide array of technologies with varying degrees of maturity. The National Quantum Initiative Act (NQI Act) in the U.S. defines the term quantum information science as the "use of the laws of quantum physics for the storage, transmission, manipulations, computing, or measurement of information."

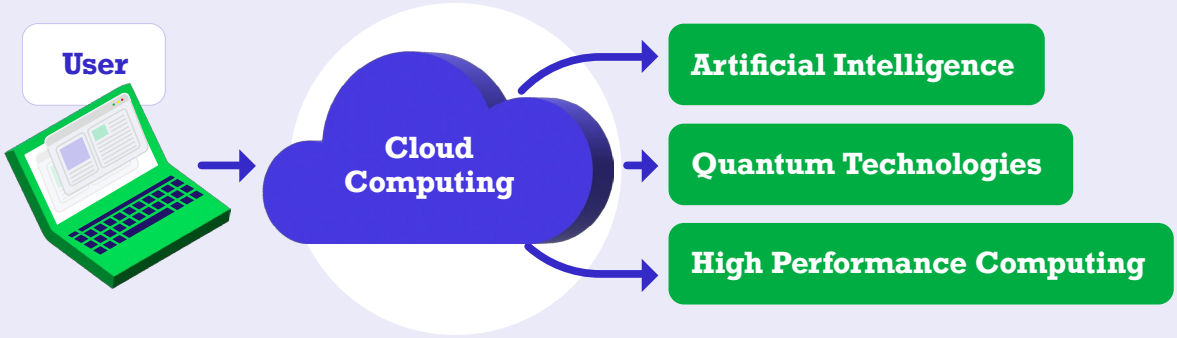
Quantum Technology Classifications

- **Quantum Computing:** Quantum Computing is a type of computation that harnesses the collective properties of quantum states, such as superposition, interference and entanglement to perform calculations.[1] Quantum computers have the benefit of being able to solve exponentially complex problems in polynomial time, the so called "quantum advantage." This means quantum computers are particularly well-suited to solve "needle in a haystack" problems. As quantum computing matures further, private sector entities and researchers are developing new algorithms that will be run on quantum computers to leverage the "quantum advantage."
- **Quantum Sensing:** Quantum properties can be used to significantly enhance sensing and measurement techniques, enabling precision measurements beyond what is possible with classical physics alone.
- **Quantum Communications:** Quantum Communications refers to the use of quantum states to ensure true randomness in number selections, to communicate encryption keys to other parties and the use of quantum effects to encode a message.

Quantum technologies encompass practical applications of QIS manifested in a variety of technologies, products, and services. Quantum Technologies can be broadly classified into three classes: quantum computing, quantum sensing and quantum communications.

Quantum Technologies, High Performance Computing, and AI

The convergence of Quantum Computing, Artificial Intelligence (AI), and High-Performance Computing (HPC) is revolutionizing various domains, including scientific research, industrial applications, and commercial innovation. By combining the strengths of each field, we can accelerate scientific discoveries, optimize complex simulations, and prepare for future computational breakthroughs.



Post-Quantum Cryptography

Post-quantum cryptography (PQC), sometimes also referred to as quantum safe encryption or quantum safety, is a separate discipline from QIS. PQC describes a set of algorithms and processes that aim to protect data against the risk of being decrypted by a quantum computer. This risk stems from a proven vulnerability in widely used public key encryption algorithms. Migrating vulnerable cryptographic systems to PQC is a long-term journey that must navigate complex interdependencies. While PQC is currently the preferred way to address quantum risk in the U.S., some countries are currently prioritizing other risk management solutions rooted in quantum communications or a hybrid approach.

AI-Driven Scientific Discovery with Quantum Computing

Cloud-based platforms are emerging that integrate quantum computing, AI, and HPC to advance fields such as materials science and chemistry research. These platforms enable researchers to perform large-scale simulations and use AI to enhance the efficiency of scientific investigations. The key features of these platforms include:

- **AI-assisted workflow automation**
- **Hybrid quantum-classical algorithms for precise simulations**
- **Quantum-inspired optimization to improve problem-solving.**

Section II:
Policy Implications of Quantum Technologies

Quantum technologies have profound public policy implications, spanning issue sets including national security, economic competitiveness, cybersecurity and data privacy. Policymakers are paying close attention due to the disruptive potential offered by these technologies.

Innovations in quantum technologies hold the promise of revolutionizing a wide range of industries by leveraging quantum physics for information storage, transmission, computing, or measurement. By leveraging conventional computing and AI, companies have made significant advancements in applying the principles of quantum physics to areas like quantum computing, error correction, process optimization, information storage, and metrology. As quantum computing matures further, researchers will be able to run new algorithms to solve "needle in a haystack" problems related to areas like cybersecurity, materials science, drug development, and machine learning.

This technological progress is paralleled by substantial economic potential. Possible economic impacts span multiple sectors: quantum computers could accelerate drug discovery and material science by simulating molecular interactions faster than a classical computer, unlocking new pharmaceuticals and advanced materials.[2] Quantum computers have demonstrated initial successes in optimizing complex systems in finance, logistics and grid management. Quantum sensing devices can improve medical imaging to navigation systems, impacting industries like healthcare, mining and transportation.[2] Because of the breadth of applications, quantum computing alone is expected to generate $450 billion annually by 2035, while quantum sensing and quantum communication are expected to generate $100-200 billion and $50-100 billion annually, respectively.[3]

Annual Expected Capital Generation by 2035:

Quantum Computing:

$450 BN

Quantum Sensing:

$100-200 BN

Quantum Communication:

$50-100 BN

Source: Bogobowicz, Michael, et al. "Steady Progress in Approaching the Quantum Advantage."McKinsey & Company, 24 Apr. 2024, https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/steady-progress-in-approaching-the-quantum-advantage."

Recognizing this potential, countries view leadership in quantum technologies as an engine for future economic growth and are racing to stake out positions in the emerging quantum enabled economy. Several countries have taken a central role and are allocating substantial resources by initiating national strategies, dedicated funding programs and the formation of international partnerships. The high risk for private investors is further incentivizing governments to take a central role in nurturing quantum technology ecosystems. As of December 2023, 24 countries have some form of national initiative or strategy on quantum information sciences and global public investment is estimated to have reached $42 billion by 2024.[4] Together, these efforts reflect a global recognition that leadership in quantum technologies is a strategic imperative for national security and economic competitiveness.

China has recognized the high stakes and accounts for a large portion of the $42 billion in global public investment. This substantial financial commitment underscores China's determination to secure a leading role in the quantum technology race, highlighting the urgent need for other nations to ramp up their own investments to remain competitive and safeguard their national interests. If China becomes the first nation to achieve a fully functional quantum computer, the national security implications for other countries could be profound. Such a technological milestone would not only position China as a global leader in a cutting-edge technology but also afford it significant strategic advantages in various sectors, including defense, cybersecurity, AI, and technological innovation. The ability to solve complex problems and optimize processes at unprecedented speeds could give China a substantial edge in fields like materials science, drug development, and machine learning, bringing China closer to realizing its economic and strategic aspirations.



$42 BN

Global investment as of 2024



24

Countries with some form of national initiative or strategy on quantum information sciences

First mover advantage in quantum technologies – particularly quantum computing – can offer countries and private sector companies significant strategic opportunity including technological leadership, competitive edge and economic impact. However, these strategic advances also carry risks, such as high R&D costs, supply chain challenges, technology unpredictability and the challenge of building a skilled workforce.

In an effort to help global policymakers to balance the benefits and risks offered by quantum technologies, we offer below in Section III policy principles on which industry, government, academia, and other stakeholders can collaborate.

Key Government Backed Quantum Initiatives

In the U.S., Congress enacted the National Quantum Initiative (NQI) Act in 2018, which directs the President to develop a 10-year plan to accelerate development in quantum information sciences and technologies and invest in funding federal R&D activities and a quantum ready workforce. The Act also provides guidance to NIST, NSF, and DOE to carry out research in quantum information science. The 2022 CHIPS and Science Act authorizes the DOE to establish an Advanced Computing Program and the NSF to continue its Federal Cyber Scholarship-for-Service Program. In Aug. 2024 the Executive Office of the President tasked National Security Telecommunications Advisory Committee (NSTAC), an industry advisory body that provides the President with advice on the Information & Communications Technology (ICT) ecosystem with respect to national security, cyber, and emergency preparedness, with assessing national preparedness for the post-quantum era via a new study

Australia's Department of Industry, Science and Resources launched the Critical Technologies Challenge Program in 2023 to boost awareness and adoption of quantum technologies by connecting stakeholders to promote R&D.

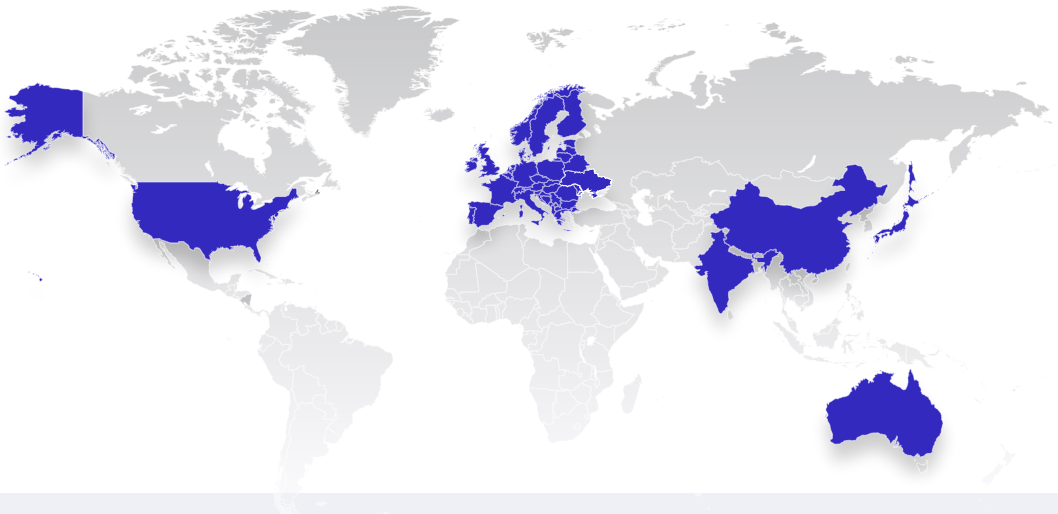
The UK's National Quantum Technologies Programme has been in operation since 2014 and is a collaboration between industry, academia and government aimed at converting quantum sciences into new products and services.

India launched the National Quantum Mission in 2023, which aims to seed, nurture, and scale up scientific and industrial R&D and create a vibrant and innovative ecosystem in quantum technologies.

The European Quantum Technologies Flagship aims to strengthen and expand European scientific leadership in R&D and to transition quantum physics from the lab to market.

Japan's Ministry of Education, Culture, Sports, Science and Technology's Quantum Leap Flagship Programme focuses on R&D on quantum simulation, computing and sensing.

China has made quantum technology a pillar of its national strategy and is investing heavily in labs and leading the world in quantum patent filings.



Section III:
Policy Principles

1 Unleash Innovation and Investment in Quantum Technologies

2 Support the Development of a Resilient Quantum Technologies Supply Chain

3 Consider the Cybersecurity and Privacy Implications of Quantum Technologies

4 Develop a Skilled Quantum Workforce

5 Adopt a Balanced Approach to Quantum Technologies Governance

6 Prioritize Global Engagement and Cooperation

1 Unleash Innovation and Investment in Quantum Technologies

As we highlight above, quantum technologies promote innovation and present enormous economic potential. Innovation and investment in quantum technologies will be critical in facilitating the development, deployment and uptake of quantum technologies. While many governments have already recognized the strategic benefits of investing in quantum technologies, they should consider developing national strategies that harness academic and private sector innovations that focus on unlocking the benefits for stakeholders across society.

Develop and support policies that incentivize private and public sector investments in quantum technologies focused R&D

We encourage robust government support to promote R&D to foster innovation in quantum technologies through incentives, increased funding and support for foundational sciences around quantum technologies, and programs that focus on commercial uses. Governments remain the primary source of funding for long-term high risk/high rewards projects in quantum technologies. We recognize that governments have launched programs that primarily support basic research in quantum technologies. Governments should continue to work with key stakeholders to refine their programs that focus on innovation, commercialization, and workforce development. Effective collaboration can be achieved through long term partnerships with the private sector and academia. A good example of this type of partnership is the Quantum Economic Development Consortium (QED-C) in the U.S. QED-C is a collaborative public-private partnership that brings together government, agencies, industry leaders and economic experts to accelerate the development and commercialization of quantum technologies. By pooling resources and expertise, QED-C aims to foster innovation, set industry standards, and advanced workforce development initiatives in the quantum technologies sector.

Governments should also consider investments that are targeted towards specific results such as quantum technology testbeds which can help bridge the gap between academic research and physical resources like hardware. In partnership with the private

sector and academia, governments should also invest in quantum focused technology centers and support grand challenges to solve specific technological challenges.

Support and promote policies that integrate quantum technologies and conventional computing, including exascale, HPC and supercomputing

Hybrid systems can leverage the strengths of both classical and quantum computing. While classical systems excel in large data processing, quantum computing has the potential to solve certain complex problems in polynomial time. Hybrid systems allow for the design of more efficient workflows, in which conventional compute solutions focus on things like the pre- and post-processing of data, whereas limited quantum computing resources are reserved for those problems that offer the quantum advantage. Accordingly, government policies that promote hybrid systems can support economic growth by spurring new industries and applications.

Support policies to build sustainable data centers for quantum innovation

To help support the advancement of quantum technologies, policymakers should prioritize the development of energy-efficient, resilient data center infrastructure. Quantum computing requires extremely low temperatures to function. Hybrid quantum workflows are also essential for building infrastructure. Investments in energy efficient powered data centers, AI-optimized energy management, and advanced cooling methods will ensure that quantum computing evolves in an environmentally responsible and commercially viable manner.

2 Support the Development of a Resilient Quantum Technologies Supply Chain

Support policies that promote – not hinder – a resilient quantum technology supply chain

Resilient supply chains are not only a business imperative for customers and companies, but critical for national security. Many foundational technologies such as semiconductors are part of complex supply chains built over decades across multiple countries. The quantum technology supply chain is no different – it is also global, highly specialized and critical for national and economic security.

Quantum technologies depend on a reliable pipeline of components, procured and sourced from all over the world. For example, rare earths are primarily mined in China; quantum photonic chipsets are designed in the U.S; specialty fiber optic cables are manufactured in Germany; dilution refrigerators are made in Finland; and advanced semiconductors are manufactured in Taiwan.

The successful development and deployment of quantum technologies will hinge on the ability to procure and produce necessary components, amongst other factors. As quantum technology grows, governments can help mitigate risks by identifying supply chain gaps, expanding quantum technology fabrication facilities and enhancing existing semiconductor fabs to develop quantum focused chips. Governments can follow existing playbooks and frameworks (e.g., NIST Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations) to manage risks while incorporating approaches that are unique to the quantum technology supply chain.

3 Consider the Cybersecurity and Privacy Implications of Quantum Technologies

Post-quantum cryptography (PQC), also known as quantum-safe encryption, is a critical field dedicated to developing algorithms and processes that protect data from being decrypted by quantum computers. The urgency of PQC arises from the vulnerability of widely used public key encryption algorithms, such as RSA, which quantum computers can decrypt in a practical amount of time. In contrast, classical computers would require millions or even billions of years to factor the large prime numbers that underpin these legacy encryption methods. Threats posed by powerful quantum computers necessitate the development of quantum-resistant algorithms and a reevaluation of current security protocols to ensure long-term data security.

Leverage existing quantum-safe solutions, especially PQC

Quantum technologies introduce both new cybersecurity threats and defensive capabilities. A sufficiently advanced quantum computer could decrypt widely adopted public key encryption algorithms, posing a significant threat to data security. Additionally, adversaries might harvest encrypted data now to decrypt it later when powerful quantum computers are deployed. To address these risks, the U.S. National Institute of Standards and Technology (NIST) has led the development of PQC algorithms. These algorithms aim to secure data against quantum-enabled attacks and enhance threat detection by identifying patterns in vast datasets more efficiently. It is worth noting, however, that these newly developed PQC algorithms are not provably secure, which means that organizations must make strategic decisions about how to handle any residual risks.

Support the development of provably secure solutions rooted in quantum communications

On the other hand, quantum communication technologies, such as quantum random number generators (QRNGs) and quantum key distribution (QKD), offer the potential for unbreakable encryption by leveraging the laws of physics to detect eavesdropping. However, these technologies are not yet available for deployment at scale and implementing these technologies will require new and specialized equipment.

Integrate quantum-safe strategies into a hybrid approach based on risk tolerance

Governments should develop nimble policies that can adapt to shifts in the cyber threat landscape. Migrating vulnerable cryptographic systems to PQC is a long-term journey that must navigate complex interdependencies. While PQC is currently the preferred way to address quantum risk in the U.S., many countries are currently prioritizing other risk management solutions rooted in quantum communications or a hybrid approach. Governments will need to make informed decisions about how best to secure their networks based on their threat tolerance and other factors.

Successful cybersecurity and privacy policies for the quantum age should encourage public and private sector stakeholders to incorporate the threat of quantum technologies into threat modeling, incident response, and information security risk management. Collaboration with key stakeholders is crucial for planning and implementing the transition to new cryptographic standards. Proactively addressing these concerns is vital for maintaining the integrity and confidentiality of digital communications in the quantum era.

4 Develop a Skilled Quantum Workforce

Support policies that will help to develop a skilled quantum technologies workforce

Governments should support policies that develop a skilled and equipped quantum workforce. The quantum technology ecosystem requires a workforce with a diverse set of skills with varying levels of proficiency. Core quantum information sciences such as quantum theory, quantum information security and quantum hardware often require high skilled expertise (master's degrees to PhDs), which governments can support by funding foundational research and development programs. At the same time, the broader quantum technology ecosystem requires a range of skills, including for engineers, technicians, applications researchers, and theoretical physicists. To help grow a workforce with these skillsets, governments should continue to pursue policies that advance education and training in STEM fields in K-12 and beyond.

Undertake studies to understand quantum workforce needs

Since most quantum technologies are in the early stages of development and remain contingent on continued technological breakthroughs, governments should undertake studies to get a more complete understanding of workforce needs. The private sector and universities can partner with governments to gain a better understanding of the education and training landscape to promote a quantum technology ready workforce.

5 Adopt a Balanced Approach to Quantum Technologies Governance

We recommend that when governments consider regulating quantum technologies, they do so in a way that balances mitigating and preventing specific harms while allowing for innovation. Quantum technologies are not a monolith and comprise different fields including computing, sensing and communications. Each field presents unique benefits and risks. Below we offer three recommendations comprising a balanced approach to quantum regulation and governance:

Adopt a risk-based, context-specific approach to governing quantum technologies

Risks related to quantum technologies need to be identified and mitigated in the context of the specific quantum technology use. Quantum sensing may pose different risks compared to quantum computing and policymakers must understand that distinction before imposing prescriptive approaches that may stifle innovation. For example, quantum sensing devices can detect electromagnetic, acoustic and gravitational signals with greater precision which could enable monitoring of activities by seeing through materials. A risk based, context-specific approach will be the most effective means of addressing concerns that may be associated with certain uses of quantum technologies as this approach can best identify specific risks while allowing for innovation.

We recommend policymakers consult industry and other stakeholders to identify high-risk use cases of quantum technologies. Similar to ITI's position on high risk in the context of AI technologies, we consider quantum technology use as high risk when a negative outcome could have a significant impact on an individual or group's health, safety, freedom or other fundamental human rights.

As use cases, benefits and risks of quantum technologies continue to emerge, policymakers should consider the OECD's Framework for Anticipatory Governance of Emerging Technologies[5] to inform and mitigate risks and promote innovation of quantum technologies.

Evaluate existing laws and regulations to determine whether new rules are required for quantum technologies

Quantum properties and principles have applications across various technologies and sectors, and stakeholders should evaluate use and impact based on specific applications. Governments should evaluate whether existing laws under consumer protection, cybersecurity and privacy/data protection address possible concerns. Quantum-specific laws run the risk of being overbroad and possibly disproportionate to addressing identified risks. Government should work with industry, academia and other stakeholders to focus potential rules and regulations to address clear harms arising from specific uses cases of quantum technologies. Prior to drafting legislation or regulations, policymakers should consider supporting industry development of, adopting, and promoting international standards which can inform the advancement of effective laws and regulations.

Align around common definitions and scope for quantum technologies

Government should strive to work towards common and consensus definitions on technical terms surrounding quantum technologies. We compile a set of definitions in the Glossary for your reference.

6 Prioritize Global Engagement and Cooperation

Countries around the world are considering developing and deploying quantum technologies. Collaboration and cooperation are key to ensuring approaches are interoperable and aligned to the greatest extent possible. We recommend governments consider the following:

Recognize the need for global cooperation and coordination

Recent trends in international science and technology collaboration showcase the balance between maintaining strategic autonomy and fostering global cooperation. National governments have been investing in quantum sciences for many years now, driven in large part by the potential digital security risks and military applications. While industry recognizes the security imperatives of countries to add safeguards for quantum and other critical and emerging technologies, realizing beneficial uses and mitigating risks is a collaborative process which is global and interdependent by nature. Coordinating funding initiatives across countries can help reduce duplication of R&D activities and help accelerate necessary breakthroughs.

International collaboration in quantum science and technology is important for both innovation and risk mitigation. A structured framework for cooperation amongst like-minded countries should emphasize joint software development to ensure interoperability. Such an initiative would not only advance quantum application across countries but would also enhance workforce development by facilitating knowledge exchange and standardizing best practices.

Groups such as the World Economic Forum (WEF) Quantum Economy Network, the Quantum Development Group, and the Multilateral Dialogue on Quantum can play an important function in coordinating the works of policymakers, technical experts, academia and industry. The OECD can also play a significant role of convener by producing reports on quantum technologies through their Global Forum on Technology and Digital Policy Committee.[6]

Support global, voluntary, harmonized standards

Standards play an important role in improving the trust of quantum technologies and promoting harmonization. They can inform potential regulations, provide guidance on governance, and support technical requirements. Governments should work towards supporting global, voluntary, industry led standards and safeguard the work and processes of international standards development bodies.

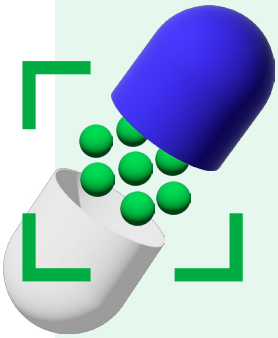
Recognizing the need to have a coordinated standards approach for quantum technologies, the International Electrotechnical Commission (IEC) and the International Organization for Standardization (ISO) announced in January 2024 the establishment of a joint committee on quantum technologies (ISO/IEC JTC 3, *Quantum Technologies*)[7]. The scope of this ISO/IEC joint technical committee is to develop standards in quantum computing, quantum simulation, quantum sources, quantum metrology, quantum detectors, and quantum communications.

Develop policies that collectively advance national security, economic security and quantum competitiveness

Export controls, technology transfer guidelines, investment screening, and other economic security measures represent critical policy tools for managing the dual use nature of quantum technologies. Governments should support policies that strike a delicate balance between domestic innovation and safeguarding sensitive technological capabilities with potential military applications. In order to balance innovation and security, governments should consider adopting policies that allow for collaborations among trusted allies and institutions with robust security measures, rather than imposing blanket restrictions that hamper scientific progress. Policymakers and regulators should also establish a transparent and predictable licensing process for quantum technologies that may be subject to export controls. For more information regarding economic security measures impacting quantum and other emerging technologies, please see *ITI's Policy Recommendations for U.S. Economic Security*.[8]

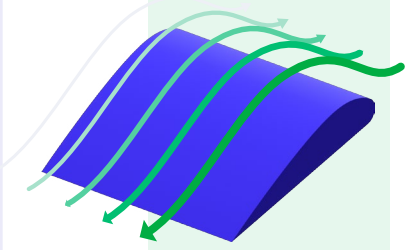
Section IV:
Quantum Technology Use Cases

While still at varying stages of maturity, quantum technologies are already in daily use. Quantum technology capabilities continuously meet milestones and some have produced initial commercial success stories while others still lack maturity for large scale commercial applications. Companies leverage quantum physics for information storage, transmission, computing, or measurement. By leveraging conventional computing and AI, companies have made significant advancements in applying the principles of quantum physics to areas like quantum computing, error correction, process optimization, information storage, and metrology.



Drug Discovery[9]

Quantum computers have been deployed towards healthcare research with an aim to help accelerate biomedical discoveries. Quantum computing, AI, and hybrid cloud technologies are also being leveraged to expedite biomedical research. These initiatives include the development of quantum computing pipelines for drug screening and optimization, the enhancement of quantum-assisted prediction models for cardiovascular risk, and the application of AI to analyze genome sequencing data and drug-target databases to identify potential treatments for diseases like Alzheimer's.



Materials Sciences[10]

Commercial aircraft are built using advanced ply composites, which are lightweight, strong, and fuel-efficient. However, designing aircraft components with these materials is highly complex, as each component consists of thousands of layered plies, each with a specific orientation to maximize strength. Determining the optimal arrangement can involve managing up to 100,000 variables – too many for classical computers to solve all at once. Engineers currently break the problem into smaller pieces, solving each separately before integrating them, a process that ensures safety but adds time and cost.

Quantum computing offers a potential breakthrough for this challenge. While current quantum systems are not yet powerful enough to optimize an entire aircraft component, as quantum hardware advances, it could enable engineers to solve large-scale optimization problems more efficiently, leading to faster, safer, and more cost-effective aircraft design.



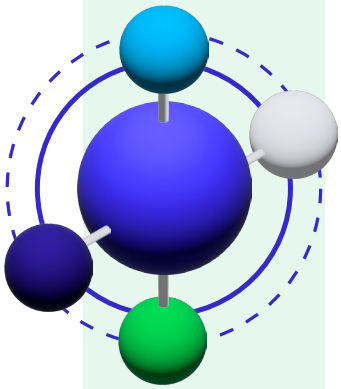
Improving Government Efficiency[11]

Quantum computing has the potential to improve government operations by solving complex problems that classical computers often struggle with. Many government functions – such as traffic management, supply chain logistics, and resource allocation – require analyzing vast amounts of data and optimizing multiple variables simultaneously. Quantum computers have the potential to process these complex calculations exponentially faster than traditional systems, enabling governments to develop more efficient urban planning, optimize energy grids, and enhance cybersecurity protocols. Quantum innovations in these areas could lead to smarter infrastructure, reduced costs, and improved public services.



Post-quantum Cryptography

Companies across sectors have begun deploying PQC algorithms to modernize cryptographic systems and to protect critical information and communication systems. To prepare and adapt cryptographic methods, organizations need to survey, inventory, and re-evaluate current security protocols. Proactively addressing concerns is crucial for maintaining the integrity and confidentiality of digital communications in the quantum era. Financial organizations are migrating to PQC to secure essential processes such as payments, digital interactions with customers, and communications with market infrastructure. Organizations have also successfully secured multi-orbit communications using PQC where they delivered crypto-agile quantum-resilient channels from earth to a low earth orbit (LEO) satellite to a geosynchronous orbit (GEO) satellite and back down to earth. This approach can build redundancy in the event of breach, failure or threat to satellites in a single orbit.



Synergistic Potential of Quantum Computing, High Performance Computing and AI in Catalysis Research

Recent efforts have demonstrated the synergistic potential of AI, HPC, and quantum computing in analyzing catalytic reactions. By leveraging logical qubits to enhance quantum simulations and conducting large-scale density functional theory (DFT) calculations, researchers can model chemical interactions with greater precision. Key findings include:

- **Mapping thousands of molecular configurations for reaction networks**
- **Successful implementation of hybrid quantum-classical workflows**
- **Potential applications in drug development and industrial catalysis**

This research highlights the promise of AI-driven quantum chemistry to uncover new materials and reaction pathways that were previously beyond the reach of classical methods alone.

Section V:
Glossary

Classical Computers: A classical computer is a device that processes information using classical physics principles, employing bits as the fundamental unit of data, where each bit represents a state of either 0 or 1.

Entanglement: Entanglement occurs when two quantum objects are so strongly correlated that they are described by the same wavefunction. Superposition states of multiple quantum objects, such as pairs of electrons or photons, are entangled if they cannot be separated into two individual wavefunctions.[12]

DiVincenzo Criteria: Refers to a set of five minimum requirements that a qubit technology must have in order to be considered a viable candidate for quantum computing. Criteria include scalability, ability to initialize a qubit state, qubit coherence times, universal gate set, and qubit measurement.

High Performance Computers: High-performance computers (HPCs) are advanced computing systems designed to perform complex calculations at extremely high speeds. They are used for tasks that require substantial computational power, such as scientific simulations, weather forecasting, molecular modeling, and large-scale data analysis. HPCs typically consist of multiple processors working in parallel, high-speed interconnects, and large amounts of memory and storage to handle intensive workloads efficiently.

Quantum Computing: Quantum Computing harnesses the quantum behavior of atoms, molecules and nano electronic circuits for a radically different and more fundamentally powerful way of computing.[13]

Quantum Communications: Quantum communications is the exchange of certain information between two or more systems that cannot be operationally accomplished with classical information exchange.[14]

Quantum Interference: Interference happens when two or more waves meet. Their highs and lows can build on one another, (constructive interference) or cancel each other out (destructive interference).[15]

Quantum Information Science (QIS): QIS refers to the application of quantum physics principles for the storage, transmission, manipulation, computing or measurement of information.[16]

Quantum Key Distribution (QKD): QKD refers to a family of protocols that generate secret keys for two or more parties in a secure way. Theoretically, security of the key distribution is guaranteed by the laws of quantum mechanics.[17]

Quantum Parallelism: Quantum Parallelism is a fundamental concept in quantum computing that harnesses the principles of quantum superposition and entanglement to execute multiple computations simultaneously, thereby exponentially increasing computational power.[18]

Quantum Random Number Generator (QRNG): A QRNG is a technology that uses the principles of quantum mechanics to generate truly random numbers, which are essential for creating secure cryptographic keys. Unlike traditional random number generators, QRNGs harness quantum phenomena to ensure that the random numbers produced are entirely unpredictable.

Quantum Sensing: Quantum sensing leverages principles of quantum mechanics, such as superposition and entanglement to achieve highly sensitive and precise measurements of physical quantities.[19]

Quantum Superposition: Quantum superposition describes a single quantum state that has characteristics of 0 and 1 at the same time. Contrary to classical computers, quantum computers are no longer bound to binary logic. Superposition states are commonly visualized using the Bloch sphere – state of a quantum system before measurement to learn about the outcome of an experiment. Superposition allows quantum computers to compute with quantum probabilities.

Qubits: A qubit, or a quantum bit, is any bit made out of a quantum system, like an electron or photon. Just like classical bits, a quantum bit must have two distinct states: one representing "0" and one representing "1". Unlike a classical bit, a quantum bit can also exist in superposition states, be subjected to incompatible measurements, and even be entangled with other quantum bits.[20]

Qubit Modalities: There are several quantum mechanical two-level systems that potentially could serve as qubits. Each system has its own unique characteristics and companies prefer different modalities for their individual purposes. Some of the best-known types of qubit modalities include superconducting qubits, trapped ion qubits, quantum dot qubits, topological qubits, diamond nitrogen-vacancy center qubits, nuclear magnetic resonance qubits, photonic qubits, and neutral atom qubits.

Uncertainty: Uncertainty tells us that pairs of properties (such as position and momentum) cannot both be known at the same time beyond an arbitrary level of precision. The act of measurement inherently changes the properties of a particle. Consequently, results can only be probabilistic expressions of likelihood. For example, we can only know where a particle is or where it is moving, but not both. Measuring the position of a particle changes its momentum and vice versa.

References

1 https://www.cigionline.org/articles/quantum-technology-national-security-and-defence-spending-a-new-frontier/#:~:text=As%20a%20dual,with%20their%20speed%20and%20capacity

2 https://www.cigionline.org/articles/quantum-technology-national-security-and-defence-spending-a-new-frontier/#:~:text=As%20a%20dual,with%20their%20speed%20and%20capacity

3 https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/steady-progress-in-approaching-the-quantum-advantage

4 https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/steady-progress-in-approaching-the-quantum-advantage

5 https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/04/framework-for-anticipatory-governance-of-emerging-technologies_14bf0402/0248ead5-en.pdf

6 https://www.oecd.org/en/publications/a-quantum-technologies-policy-primer_fd1153c3-en.html

7 https://www.iso.org/committee/10138914.html

8 https://www.itic.org/documents/general/ITI_Economic-Security-Recommendations_022425FINAL.pdf

9 https://newsroom.ibm.com/2023-03-20-Cleveland-Clinic-and-IBM-Unveil-First-Quantum-Computer-Dedicated-to-Healthcare-Research

10 https://www.ibm.com/quantum/blog/boeing-case-study

11 https://www2.deloitte.com/us/en/insights/industry/public-sector/future-of-quantum-technology-public-sector.html; https://utimaco.com/news/blog-posts/how-leverage-opportunities-and-prepare-threats-quantum-computers-government-sector

12 https://uwaterloo.ca/institute-for-quantum-computing/resources/quantum-101/glossary#C

13 https://uwaterloo.ca/institute-for-quantum-computing/resources/quantum-101/glossary#C

14 https://www.nist.gov/pml/productsservices/quantum-networks-nist/quantum-networks-nist-glossary#quantumcommunications

15 https://uwaterloo.ca/institute-for-quantum-computing/resources/quantum-101/glossary#C

16 https://www.quantum.gov/wp-content/uploads/2022/08/NQIA2018-NDAA2022-CHIPS2022.pdf

17 https://www.nist.gov/pml/productsservices/quantum-networks-nist/quantum-networks-nist-glossary#quantumcommunications

18 https://quantumexplainer.com/quantum-parallelism/

19 https://quantumzeitgeist.com/what-is-quantum-sensing/

20 https://uwaterloo.ca/institute-for-quantum-computing/resources/quantum-101/glossary#C

ITI

Promoting Innovation Worldwide

The Information Technology Industry Council (ITI) is the premier global advocate for technology, representing the world's most innovative companies. We promote public policies and industry standards that advance competition and innovation worldwide.