QUANTUM TECHNOLOGY FOR THE DEVELOPMENT OF HUMANITY

AUTUMN 2025

INTRODUCTION

Quantum technology is no longer confined to physics laboratories. It has become a strategic issue for business leaders, governments, and society at large. With the declaration of 2025 as the "Year of Quantum Technology" by the United Nations, this emerging field is gaining global attention as a driver of innovation and a potential disruptor of existing systems.

In this paper, we summarize the key insights presented during the 28th CSTD Side Event organized by the **Diplomatic Council Quantum Leap Initiative**. The initiative, operating under ECOSOC status, seeks to promote quantum technologies for the benefit of humanity, particularly underserved communities

Two leading experts, **Harald Summa** and **Matthias Reidans**, shared their experience and strategic perspective on the societal, technological, and ethical dimensions of quantum technologies. Their talk addressed:

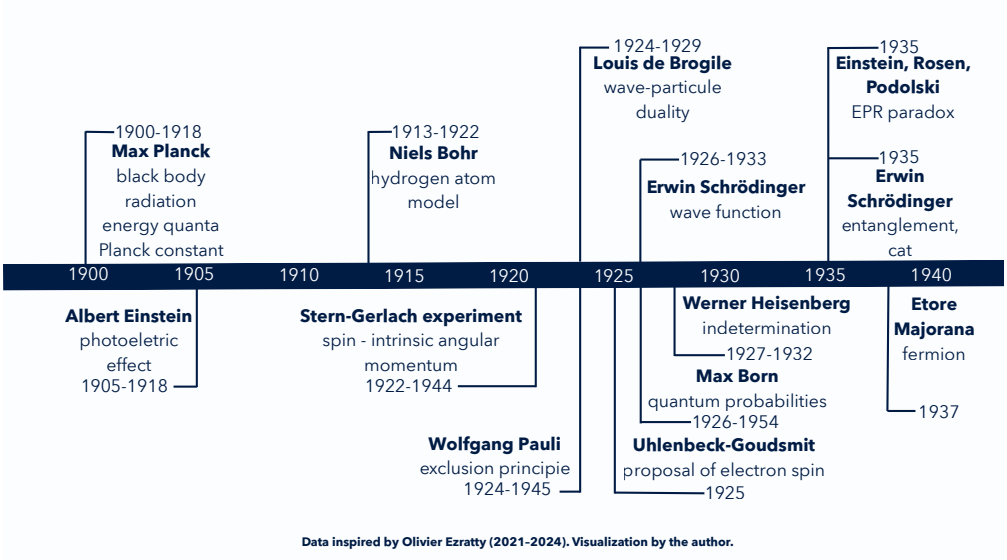
- **the evolution of quantum computing,**
- **current capabilities and limitations,**
- **its role in AI, cryptography, sensing, and infrastructure,**
- **and the need for international governance and ethical foresight.**

Internet architect, visionary, thought leader: Harald A. Summa is the founder, former CEO, and honorary president of eco – Association of the Internet Industry. From 1996 to 2022, he managed DE-CIX, the world's largest Internet exchange, and has since served on its supervisory board. In 2013, he was appointed as a core member of the advisory board of the German Federal Ministry for Economic Affairs' "Young Digital Economy" initiative, joined the advisory board for the "Digital Economy NRW," and became a member of the "Council for Digital Ethics" of the state of Hessen.

Matthias Reidans brings over 25 years of experience in the IT and datacenter industry, with a strong focus on cloud migration, infrastructure modernization, and digital transformation. He has led strategic projects for IBM, tecRacer, and currently at Rosenberger-OSI, where he is a **key expert in datacenter transformation and quantum infrastructure**. He is actively involved in promoting responsible applications of quantum technologies in enterprise contexts and is recognized as a driving force at the intersection of deep tech and real-world implementation.

WHY QUANTUM NOW?

We are entering the third quantum revolution – a time in which quantum technology is moving from theoretical physics into practical, impactful applications. While the foundations were laid over 100 years ago by pioneers like Heisenberg, Planck, and Schrödinger, it is only today that the full power of these discoveries begins to unfold in business, science, and geopolitics.



Data inspired by Olivier Ezratty (2021–2024). Visualization by the author.

The United Nations has declared 2025 the official "Year of Quantum Technology," emphasizing its relevance for sustainable development, digital sovereignty, and ethical governance. As highlighted by Sir Peter Knight during the UNESCO ceremony:

"We need all of you to change the world with quantum."

The Diplomatic Council has launched the Quantum Leap Initiative to raise awareness and foster responsible innovation. The initiative emphasizes that quantum computing should not only benefit highly industrialized countries but also less privileged societies.

Quantum technology is already impacting sectors such as **climate research, medical diagnostics, material science, AI, and cybersecurity**. This technology is not a distant promise – it is unfolding now, and early preparation determines who will lead or lag behind.

The road ahead: Quantum computing is no longer a futuristic concept – it is an emerging business and policy imperative. The next 5–10 years will decide who shapes and who follows in the quantum economy.

THE THREE QUANTUM REVOLUTIONS

From fundamental discovery to societal transformation

Over the past century, quantum theory has progressed through **three transformative phases**, each representing a leap in understanding and capability. Together, these revolutions form the **foundation for today's emerging applications** – and tomorrow's breakthroughs.

The First Revolution (1900s–1930s: Foundational Theory)

The first revolution began in the early 20th century, when pioneers such as Max Planck, Albert Einstein, Werner Heisenberg, and Erwin Schrödinger introduced the principles of quantum mechanics. They defined the mathematical and conceptual frameworks that underpin quantum theory today – including **superposition**, **wave functions**, and the **uncertainty principle**.

This era was purely theoretical, but its consequences became visible over time in fields such as lasers, semiconductors, and medical imaging.

The Second Revolution (1970s–1990s: Experimental Proof & Early Engineering)

The second revolution emerged when **quantum entanglement**, once a philosophical thought experiment, was **proven in the lab**. Researchers such as **John F. Clauser, Alain Aspect**, and **Anton Zeilinger** demonstrated that particles can exhibit non-local connections – a fact that would soon shape communication and computing.

These experiments laid the groundwork for quantum teleportation, quantum key distribution, and quantum sensing. The Nobel Prize in Physics in 2022 recognized this achievement, marking entanglement as not only real, but technologically usable.

"Entanglement is not just a curiosity – it's now an engineering tool."

The Third Revolution (2020s-ongoing: Applied Quantum Information & New Physics)

Today we stand at the **beginning of a third revolution**. Quantum computing is now being applied to real-world problems – and simultaneously, the boundaries of quantum theory are being pushed into new domains of physics, such as quantum gravity and black hole information theory.

A central concept in this phase is the ER = EPR hypothesis, proposed by Maldacena and Susskind, suggesting that entanglement may be linked to wormholes (Einstein-Rosen bridges).

This convergence of computing, physics, and cosmology may not yet be practical – but it points toward future systems that are radically beyond classical paradigms.

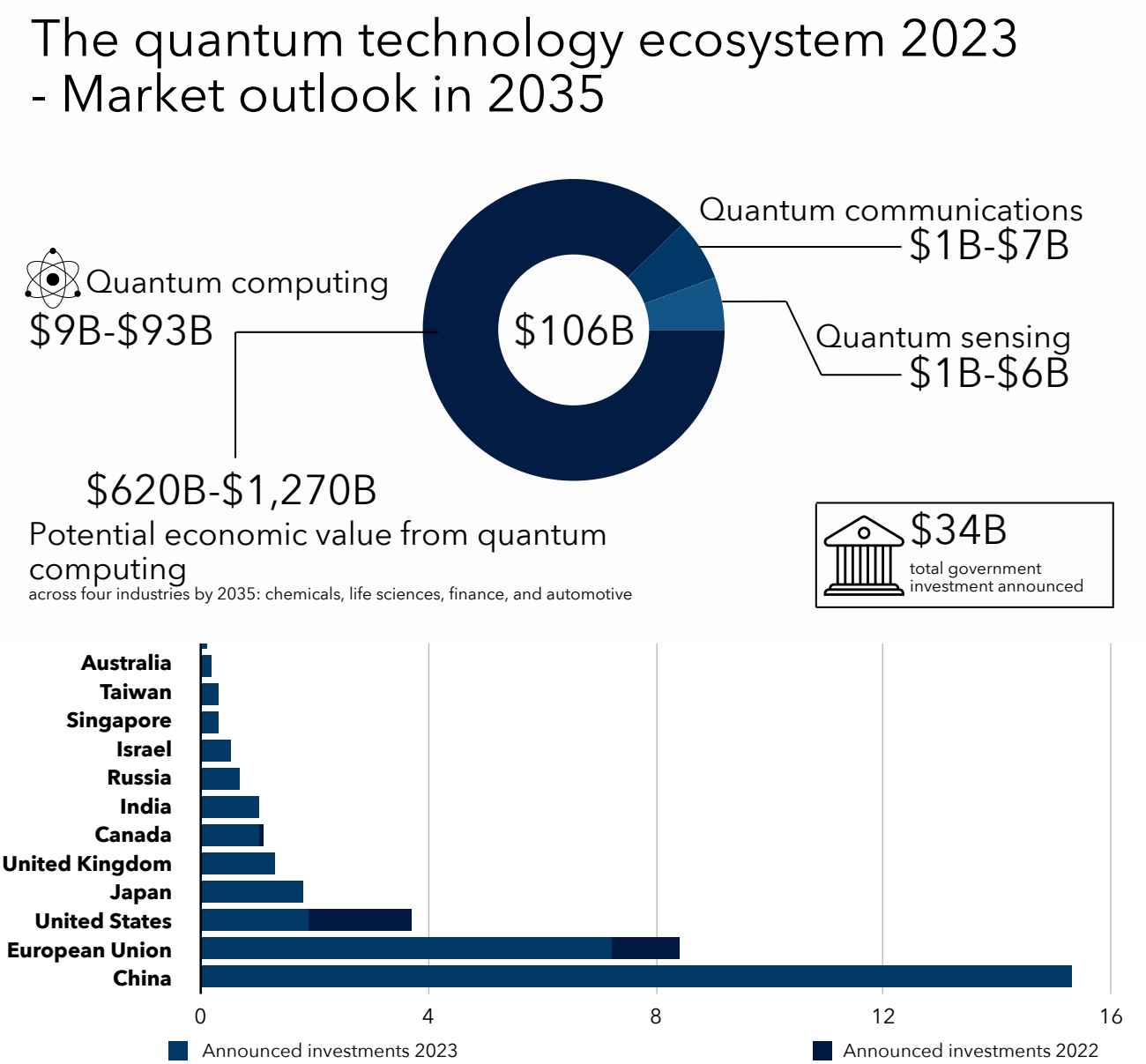
Monitor the third quantum revolution closely – it could redefine our understanding of space, time, and computation.

Business Relevance

Why it matters:

The evolving quantum revolution is no longer purely academic. It now accompanies and translates into real world applications alongside theoretical research.

- Quantum effects can now be engineered
- Governments are competing globally
- Strategic early movers will gain technological and economic leadership
- Industry is investing:



Source: McKinsey & Company (2023). Quantum Technology Monitor – April 2023. The original data has been adapted and visualized by the author. The full report is available at: www.mckinsey.com

TECHNOLOGICAL STATUS 2025

Where are we now – and what still holds us back?

Quantum computing is no longer confined to theory or lab prototypes. In 2025, companies across sectors are beginning to experiment with practical use cases, often through quantum cloud services and early-stage hardware integrations. Yet despite this visible progress, the field still faces fundamental limitations, particularly in stability, error correction, and scalability

Hardware: Progress, But Not Yet Precision

Current quantum systems use a variety of physical platforms. Among the most prominent are superconducting qubits, employed by companies like IBM and Google, which use electrical currents at near-zero temperatures to generate qubit states. Another well-established approach is based on trapped ions, utilized for example by IonQ and eleQtron, where charged atoms are suspended and manipulated with laser pulses.

Other approaches include nitrogen-vacancy (NV) centers in diamond, which are particularly attractive due to their optical accessibility and potential for room-temperature operation. Additionally, cold atoms and photonic chips offer scalable architectures with potentially lower error rates, although they remain technically challenging and are still largely in the experimental phase.

Each platform offers trade-offs in terms of coherence time, scalability, and noise sensitivity. The field has not yet converged on a dominant architecture. Most systems remain highly experimental, with only dozens or a few hundred usable qubits – far from the millions needed for fault-tolerant applications.

"Quantum computers in future are like Formula 1 race cars with 300,000 horsepowers but chassis, tires and tracks aren't prepared any how."

Software and Interface: New Coding Paradigms Needed

To operate quantum computers, developers rely on specialized programming frameworks tailored to quantum logic. One of the most widely used is Qiskit, developed by IBM, which allows users to build and simulate quantum circuits. Similarly, JQM, developed by JoS Quantum, serves as a platform-oriented operating system that enables a quantum-adapted process workflow by abstracting hardware-specific complexity.

In addition, there is growing interest in quantum-enhanced machine learning libraries, including models based on Boltzmann machines and quantum amplitude estimation. These tools enable hybrid workflows where classical and quantum algorithms are combined – though such workflows still require high expertise and are rarely production-ready.

Despite promising demos, these toolkits are still fragmented and require deep expertise. Large-scale enterprise integration remains rare.

Cloud Access: Democratizing Quantum – with Limits

The rise of cloud-based quantum computing has opened up access for a wider range of users. These platforms help to bridge the skills gap, making it possible for non-specialists to test algorithms and experiment with quantum hardware. They also enable real-world experimentation without the need to invest in costly and sensitive infrastructure.

At the same time, quantum cloud access can significantly reduce infrastructure costs for companies, particularly in the early exploration phase. However, limitations remain – including long wait times, limited qubit availability, and the inherent instability of current devices operating in the NISQ (Noisy Intermediate-Scale Quantum) era.

Technology Snapshot 2025

Area	Current Status	Limitation
Qubit Count	50-400 (depending on platform)	Instability, noise
Commercial Use	Exploratory pilots	No fault tolerance, insufficient performance
Cloud Access	IBM or IonQ via Amazon Braket, IQM	High latency, low availability
Software	Experimental frameworks	High barrier to entry

BUSINESS APPLICATIONS OF QUANTUM TECHNOLOGY

From lab to logistics, finance, and healthcare

While the technological foundations of quantum computing are still being refined, early applications across industries are already taking shape. These use cases do not require fully error-corrected quantum computers, but leverage quantum principles to solve problems that are computationally intractable for classical systems.

Pharmaceuticals and Medical Diagnostic

Quantum computers can simulate complex molecules and protein interactions far more precisely than classical machines. This is transforming fields such as drug discovery – including research into malaria, cancer, and rare diseases – by enabling the modeling of molecular binding and protein folding. In diagnostics, quantum systems can improve early detection through pattern recognition in medical datasets. Moreover, they support the design of personalized medicine by enabling simulations of individual molecular responses.

These applications drastically shorten development timelines and reduce R&D costs. Their social impact could be immense, especially in global public health.

"This is not about computing power alone – it's about solving questions we couldn't even formulate before."

Climate Modeling and Energy Systems

In the energy sector, quantum algorithms are being tested to optimize complex systems. This includes improving power grid stability by simulating and adjusting load balancing in real time. Quantum simulations also accelerate battery material research and help model climate systems more accurately – for instance, by solving partial differential equations or optimizing energy flow across networks.

These are classic combinatorial optimization problems, where quantum techniques like Grover's algorithm and quantum annealing show potential.

Logistics and Supply Chains

Quantum computing supports the optimization of large-scale logistics networks. It enhances route planning, optimizes fleet usage, and enables the simulation of dynamic supply chains. These capabilities have already been tested in emergency logistics, disaster response, and humanitarian aid – where real-time adaptability and minimization of delays are crucial.

Cybersecurity and Cryptography

Quantum computing presents a unique duality in cybersecurity: while it threatens current encryption standards, it also introduces entirely new methods of securing data. Quantum Key Distribution (QKD), for instance, enables the secure transfer of encryption keys through quantum mechanics, making them unbreakable by any classical or quantum means. At the same time, Post-Quantum Cryptography (PQC) refers to algorithmic approaches – designed for classical hardware – that are more resistant to quantum attacks. These are crucial for securing databases, communications, and infrastructure against future threats. Additionally, emerging concepts such as tamper-proof authentication systems based on quantum randomness further expand the toolkit available to security experts.

"This is the first time in history that a communication line can be protected 100 percent."

This dual nature – being both a disruptive force and a potential safeguard – positions quantum security as one of the most strategically urgent fields for both public and private sectors.

Quantum technology is already shaping core sectors – not as a product, but as a capability. Early experimentation enables market positioning, innovation leverage, and regulatory foresight.

THE THREAT LANDSCAPE & QUANTUM SECURITY

From breaking encryption to building trust

Quantum computing doesn't just promise breakthroughs – it also threatens to break the foundation of today's digital security infrastructure. Algorithms like **RSA** and **ECC**, which protect everything from online banking to military communication, could become obsolete once scalable quantum computers reach sufficient power.

This evolving threat landscape has triggered a global race to prepare, adapt, and regulate – before the crisis materializes.

The Cryptography Time Bomb: "Harvest Now, Decrypt Later"

One of the most pressing concerns is the idea that **data is already being harvested** today – even if it can't yet be decrypted – in anticipation of future quantum capabilities. This is known as the **"Harvest Now, Decrypt Later**" strategy.

In practice, this means that malicious actors may already be storing encrypted communications with the intention of decrypting them once quantum computers become powerful enough to break RSA or ECC encryption. This includes sensitive data such as government files, corporate IP, financial transactions, and private communications. Although the encryption holds for now, once quantum systems reach the necessary scale, these past communications could be compromised retroactively.

"If quantum computing breaks today's encryption tomorrow, everything you transmit now is already at risk."

Approach	PQC	QKD
Method	Algorithm-based	Hardware-based
Tech Basis	Classical computers	Quantum communication
Infrastructure	Compatible with existing systems	Requires new optical setups
Status	NIST standardization underway	Operational in pilots, still scaling
Use case	Email, databases, software systems	Secure transmission of key data

These approaches are **not mutually exclusive** – they are complementary layers in a "**Layered Quantum Security"** model.

"You don't just build one wall. You build layers – algorithmic and physical – to protect what's critical."

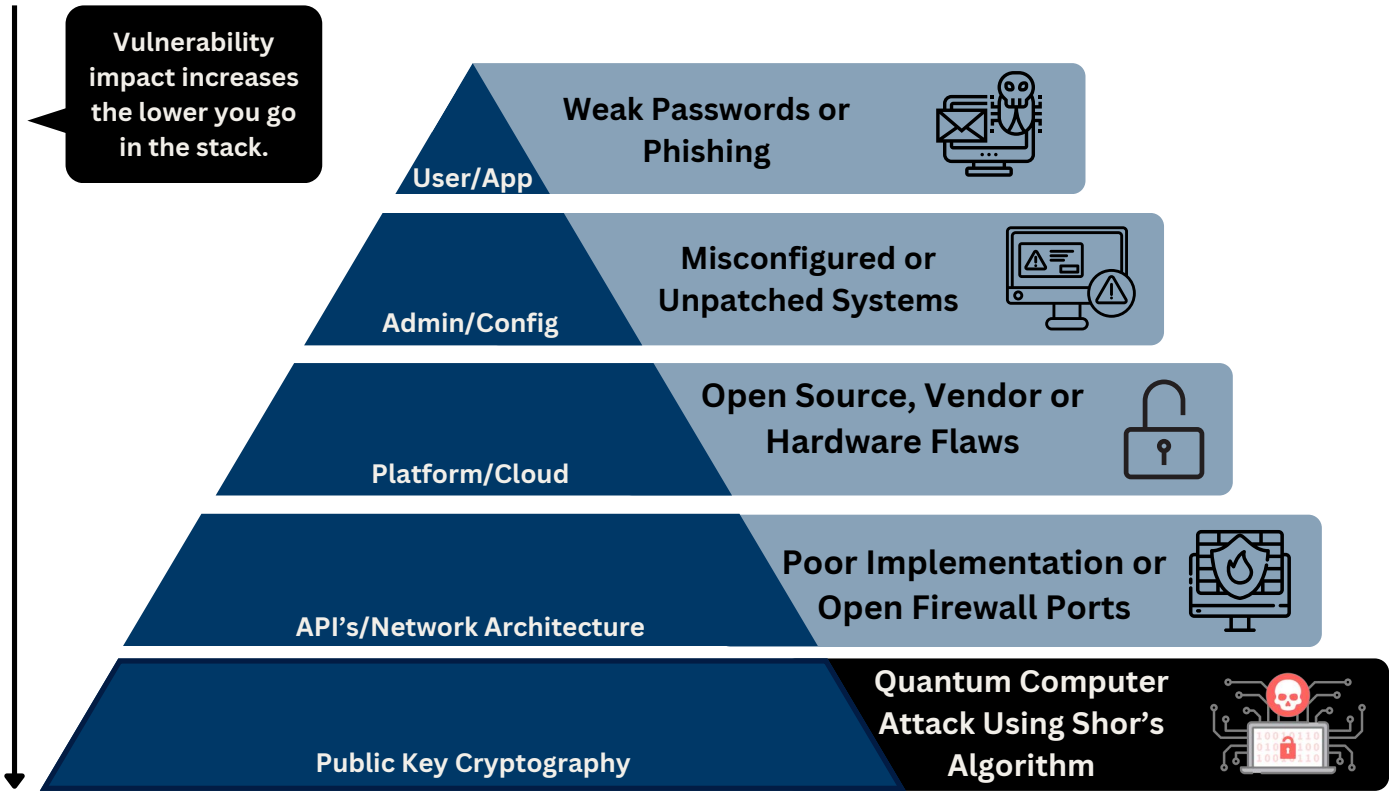
Beyond Algorithms: Trust, Identity & Systems Vulnerabilities

Quantum risks extend beyond pure encryption. As computing capabilities grow, new vulnerabilities emerge in identity verification, authentication, and hardware-based trust models. Side-channel attacks – where systems are compromised through physical leakage rather than code – may become more relevant, especially in high-security environments. Moreover, quantum technologies could outpace compliance frameworks in industries like healthcare, finance, and defense, creating legal and operational blind spots. These risks highlight the need for systemic thinking beyond mathematical cryptography.

The need for quantum-secure infrastructure now touches every layer of digital life – from local IT systems to satellites, critical infrastructure, and cross-border data regimes.

Security Layer	Description
Post Quantum Crypto	Resistant to quantum decryption attacks
Quantum Key Distribution	Enables secure transmission using quantum physics
Authentication	Stronger identity validation mechanisms
Hardware Trust	Shielding systems from physical side attacks
Governance Trust	Legal framework & audibility

What Matters Now: Quantum security isn't about preventing future problems – it's about protecting today's assets from tomorrow's technology. The cost of delay is irreversible exposure.



GOVERNANCE, ETHICS & THE COLLINGRIDGE DILEMMA

Regulating a technology before it defines the rules

Quantum technology raises not only scientific or commercial questions, but also **profound ethical and geopolitical concerns**. Its development is advancing faster than regulatory and societal frameworks can adapt – a classic case of the **Collingridge Dilemma**: When regulation is easy, the impact is unknown; when the impact is known, regulation becomes difficult.

Global Power Dynamics: The Risk of Quantum Advanatge

Quantum advantage could widen the global digital divide. Countries with early access to scalable quantum infrastructure may come to dominate key strategic areas. This includes cybersecurity, where control over secure communication protocols could determine national resilience; scientific research, where simulation capabilities may accelerate innovation unevenly; economic modeling, as quantum systems enable the forecasting and manipulation of financial markets; and defense and surveillance, where quantum sensing and intelligence tools could shift global security balances.

This raises the risk of technological monopolies, digital colonialism, and the loss of agency for developing nations. Quantum technologies must be developed with inclusivity in mind. If access is limited to a small number of economically or technologically dominant actors, the risk is that existing global inequalities will be amplified rather than addressed.

Ethical Uncertainty: From Surveillance to Social Impact

Quantum's capabilities could be misused in several sensitive domains. Mass surveillance may be enhanced by quantum-assisted data analysis and pattern recognition. Predictive policing algorithms could be trained on quantum-processed datasets, raising questions about bias and civil liberties. Autonomous military systems might incorporate quantum sensors or cryptographic tools, leading to new forms of warfare. And the manipulation of economic systems – such as influencing stock markets or supply chains – could become more opaque and difficult to regulate.

These concerns are not speculative – they are already on the policy radar of the EU, UNESCO, and independent institutes like ITAS in Karlsruhe, Germany.

Dual-Use Risk: Learning from the Nuclear Age

The history of nuclear technology offers a stark reminder: **breakthroughs intended for progress can become instruments of destruction** if governance lags behind.

Quantum systems, particularly in cryptography, sensing, and simulation, have already attracted interest from defense sectors. Without early transparency and enforceable treaties, we risk developing **the quantum equivalent of the atomic bomb** – with geopolitical implications we are not prepared to manage.

The lesson from nuclear history is clear: **the first to build power often shapes the rules – and the weapons.**

International coordination must begin now, not after the first irreversible misuse. Ethical foresight is not just a moral duty – it is a form of strategic stability.

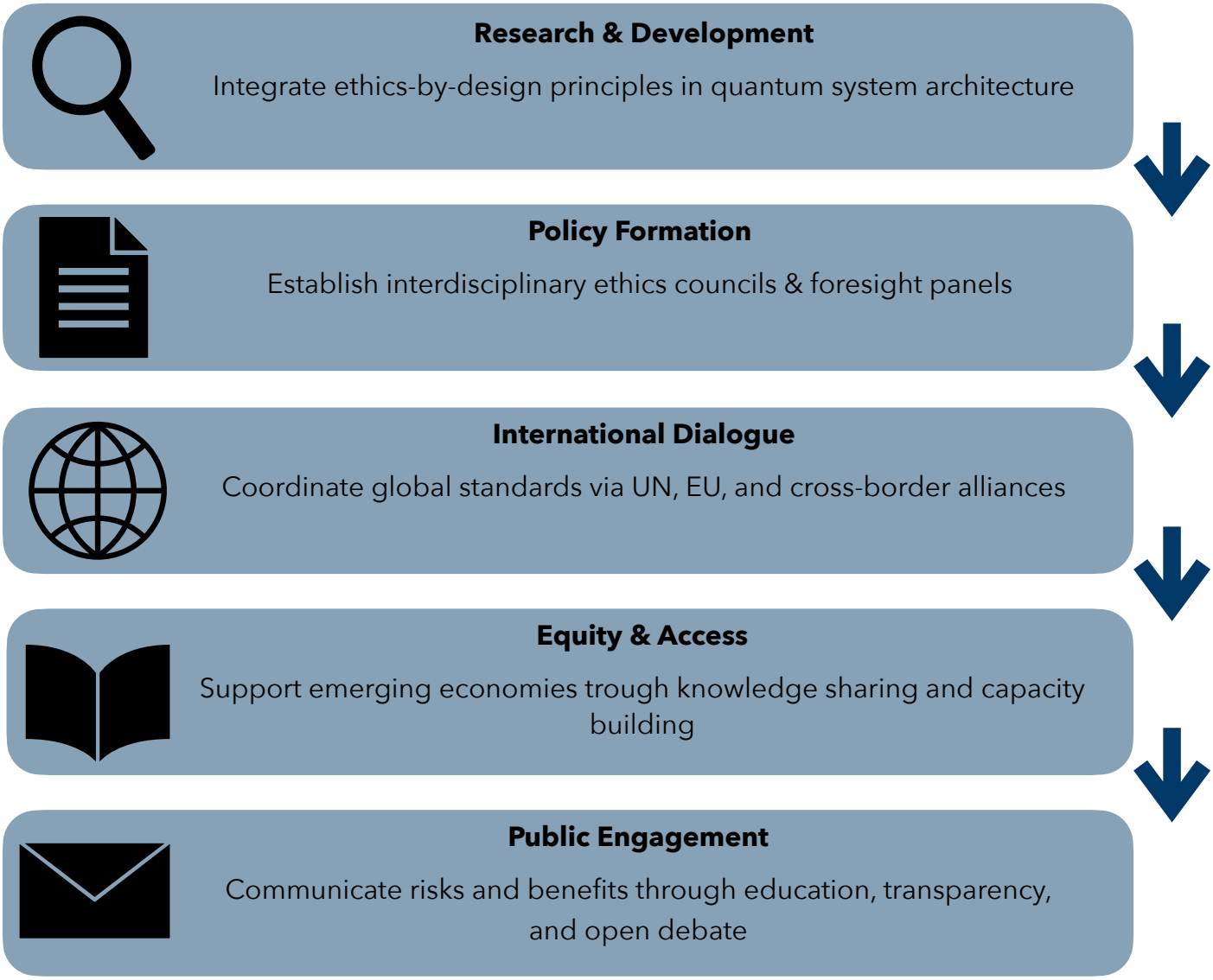
Lessons from the Past: What Nuclear, AI & Genetics Teach Us

The ethical history of past technologies like nuclear energy, genetic editing, and artificial intelligence offers clear warnings for quantum policy. In each case, early enthusiasm for transformative potential – clean energy, medical breakthroughs, or intelligent automation – was followed by ethical dilemmas such as weapons development, biosecurity risks, or systemic bias. Only then did regulatory responses emerge, such as the Non-Proliferation Treaty, CRISPR oversight boards, or the EU AI Act.

Quantum technology must not follow the same reactive pattern. Proactive ethical guidance is essential to avoid repeating cycles of harm-mitigation after deployment. The goal should not be to respond to risk once it appears, but to anticipate and embed accountability while the technology is still forming.

Key Recommendations for Ethical Quantum Governance

To guide ethical governance, the follow roadmap outlines the core domains for anticipatory regulation and global coordination.



STRATEGIC RECOMMENDATIONS FOR BUSINESSES & POLICYMAKERS

Preparing today for a quantum-powered tomorrow

As the quantum landscape evolves, organizations must not wait for fully scalable systems before they act. Instead, they should develop **capabilities, governance strategies, and talent pipelines** that position them for future adoption.

Prioritize Quantum Readiness – Not Immediate ROI

Quantum computing today offers no plug-and-play advantage. However, companies that experiment early gain a number of strategic benefits.

They acquire internal know-how through practical exposure and internal training initiatives. By being part of early development cycles, they help shape industry standards and norms. They also gain a first-mover position in establishing intellectual property rights around emerging use cases. Finally, early actors can influence upcoming regulatory frameworks by participating in pilots, sandboxes, or consortia.

"This is about learning before leveraging. You don't wait until the rules are set – you help write them."

Transition to Post-Quantum Cryptography (PQC) Now

With classical encryption under long-term threat, organizations should begin the transition toward quantum-resilient infrastructure.

This includes auditing their current cryptographic systems to identify vulnerable protocols, adopting NIST-recommended PQC algorithms that are designed to withstand quantum attacks, and implementing hybrid encryption strategies that combine classical and quantum-safe elements. These measures ensure continuity and confidentiality, even as threat models evolve.

Invest Quantum-Aware Talent

This ensures data confidentiality even under future quantum attacks. Quantum development needs cross-disciplinary skills, as outlined in the adjacent table.

Role	Skillset Requires
Quantum engineers	Physics, hardware control, noise management
Quantum developers	Gate logic, quantum algorithms, toolchains
Strategy leads	Market readiness, regulatory mapping
Compliance officers	Risk profiling, PQC adoption, crypto hygiene

"Quantum is not only about tech talent – it's about leaders who can ask the right questions."

Support Global Alignment & Collaboration

Businesses and policymakers must actively engage in international coordination. This includes participating in the development of global standards through institutions like ISO, ETSI, and NIST. Collaboration with public-private consortia – such as the DC Quantum Leap Initiative or the EU Quantum Communication Infrastructure – also plays a key role. Finally, governments and industry stakeholders must engage in international diplomacy to address dual-use concerns and avoid fragmented quantum governance.

Strategic Quantum Actions

Domain	Action Item
Cybersecurity	Inventory encryption
Workforce	Upskill teams in quantum foundations
R&D	Join pilot programs or sandboxes with tech partners
Governance	Embed quantum ethics into tech evaluation processes
Policy	Participate in national or EU-level or globally settled strategy frameworks

FINAL OUTLOOK & CALL TO ACTION

Responsibility, resilience, and readiness in the quantum age

Quantum technologies are not emerging in isolation. They are arriving in a world already grappling with inequality, fragmented trust, and growing geopolitical uncertainty. What sets quantum apart is not just its technical novelty, but the profound impact it could have on the structural foundations of our societies – from how we process information to how we govern, protect, and collaborate across borders.

From encryption and AI to global communications and fundamental physics, quantum computing will influence not only individual systems but the logic behind those systems. This makes it fundamentally political – and ethically charged.

This transformation cannot be left to chance. The experts in this session – and the broader quantum research and policy communities – have made one point abundantly clear: the time to act is now. Waiting until quantum advantage is fully realized would mean being too late to shape its governance, too late to secure critical systems, and too late to ensure that its benefits serve the many, not the few.

We are in a brief but critical window where influence is still possible. We are not just building machines – we are building the conditions for future societies.

Strategic Fields of Action for the Quantum Age

How governments and businesses can lead – not react

To meet this moment, five strategic priorities should guide public and private decision-making.

First, quantum security threats must be addressed not as distant hypotheticals, but as concrete risks. This means building realistic transition paths now – from crypto audits to PQC adoption – to ensure that current data and systems remain secure even as quantum capabilities grow.

Second, access and talent must be democratized. Inclusion is not an ethical luxury – it is a functional necessity. A quantum future dominated by a few actors risks replicating or worsening global inequalities. Empowering diverse talent pipelines and lowering barriers to participation will define whether quantum becomes a shared innovation or a fragmented advantage.

Third, collaboration must cross institutional boundaries. No single actor can govern quantum alone. Policymakers, scientists, industry leaders, and ethicists must co-create flexible frameworks that evolve with the technology – keeping innovation and regulation in dynamic balance.

Fourth, quantum must be embedded in long-term digital strategies. This is not an isolated domain. Quantum intersects with cloud infrastructure, cybersecurity, telecom, and artificial intelligence. Nations and companies that treat it as a silo will miss the compound effects it can offer – or the risks it introduces.

Fifth, the guiding principle must be foresight – not fear. The biggest threat is not overreaction, but inertia. Delaying action now means ceding control over how quantum unfolds. Acting today allows us to influence its design, purpose, and accessibility – rather than reacting to its consequences too late.

This time, we have the chance to lead with foresight – not regret.

There is a bright future ahead. But we must not ignore the clouds – they often come faster than expected.

We have already seen what happens when the quest for scientific dominance outpaces ethical alignment. The invention of nuclear weapons showed how technological power, if not governed early, can shape global history in irreversible ways. Quantum technologies, while different in nature, carry a similar dual-use risk – and an equally profound responsibility.

If we fail to anticipate how quantum systems might be used – or misused – we may once again find ourselves writing rules too late, under pressure, and without consensus.

The Closing Thought

Quantum is more than a technology. It is a mirror of how we plan, how we cooperate, and how we define progress. Its trajectory will reflect the choices we make now – whether to regulate, to educate, to invest, and to lead.

This is not about optimism versus pessimism.

It is about readiness and readiness starts today.

FURTHER INFORMATION

ABOUT THE DIPLOMATIC COUNCIL & THE QUANTUM LEAP INITIATIVE

The Diplomatic Council (DC) is a global think tank, international business network, and charitable foundation with consultative status at the United Nations Economic and Social Council (ECOSOC). Founded by diplomats and business leaders in 2012, the DC promotes economic diplomacy and fosters technology-driven solutions for peace and prosperity.

Within the framework of the UN's Agenda 2030, the DC supports initiatives at the intersection of science, business, and policy – among them, the Quantum Leap Initiative, chaired by Harald A. Summa. The initiative aims to accelerate the development of a global quantum ecosystem, comparable to the transformative impact of the internet. It promotes responsible access to quantum computing, sensing, and encryption technologies through global collaboration and public engagement.

Through its international reach, the DC actively contributes to the United Nations' science and technology agenda by organizing side events at CSTD sessions, participating in WSIS forums, and publishing thought leadership. Working groups within the initiative meet regularly online and in person to translate vision into impact.

For more Information: office@diplomatic-council.org, www.diplomatic-council.org/quantumleap

CONTACT

Andreas Dripke
Executive Chairman
Diplomatic Council (Uno reg.)

PROJECT SUPPORT

Karl Kimmig
Content Contributor & Accelerator

Vincent Schaffrin
Editorial Lead | Research & Coordination

CONTRIBUTORS & EXPERT CONTACTS

Harald A. Summa
Lead Speaker | Strategy & Governance

Matthias Reidans
Lead Speaker | Technology & Infrastructure